Journal of Law and the Biosciences, 1–36
https://doi.org/10.1093/jlb/lsab007
Original Article

Standard contractual clauses for cross-border transfers of health data after *Schrems II*

Laura Bradford*,†, Mateo Aboy‡ and Kathleen Liddell**

Centre for Law, Medicine and Life Sciences (LML), Faculty of Law, University of Cambridge, UK
*Corresponding author. E-mail: lrb4002@med.cornell.edu

ABSTRACT

Standard contractual clauses (SCCs) have long been considered the most accessible method to transfer personal data legally across borders. In July 2020, the Court of Justice of the European Union (CJEU) in *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (*Schrems II*) placed heavy conditions on their use. The *Schrems II* Court found that SCCs were valid as 'appropriate safeguards' for data transfers from EU entities to others outside the EU/EEA as long as unspecified 'supplementary measures' were in place to compensate for the lack of data protection in the third country. Data protection officers are under intense pressure to explain these measures and allow routine transfers to continue. Some authorities interpret the decision as preventing the use of SCCs to transfer personal data outside of the EU because private contracts cannot comprehensively redress gaps in national law. This article argues that these authorities are mistaken and that notwithstanding *Schrems II* SCCs can still be useful instruments for cross-border transfers. This is especially true in highly regulated contexts such as medical research. This paper traces the history of SCCs under the General Data Protection Regulation (GDPR) and shows how the CJEU in *Schrems II* misunderstood the purpose of SCCs and other Article 46

† Laura Bradford is a senior research associate in the Centre for Law, Medicine and Life Sciences (LML) at the University of Cambridge, UK where she also teaches US Corporate Law in the Masters in Corporate Law Program. She is dual qualified as an attorney in the UK and in New York. She has served as a Senior Legal Advisor for the University of Cambridge, UK. In the USA, she was an assistant professor at George Mason University Law School and a visiting associate professor at George Washington University School of Law. She graduated with honors from Stanford University Law School and Yale University.

‡ Mateo Aboy is a principal research scholar in the Centre for LML at University of Cambridge, UK.

** Kathleen Liddell is the director for the Centre for LML at the University of Cambridge, UK.

GDPR 'appropriate safeguards'. The CJEU mistakenly approached Article 46 safeguards such as SCCs as being similar to country-specific adequacy rulings under Article 45 GDPR. But unlike Article 45 adequacy rulings, SCCs were not intended to provide a stand-alone mechanism for transfer reliant on the law of the importing country. Rather SCCs provide an alternative, multi-layered standard for data protection that encompasses law, technology and organizational commitments. Their purpose is to be used in situations where legislation alone is insufficient to protect data subject rights. The European Commission's new draft SCCs support this analysis.

KEYWORDS: GDPR, privacy and data protection, cross-border transfers, EU-US Privacy Shield, standard contractual clauses, appropriate safeguards, health data, medical research

I. INTRODUCTION

Since July 16, 2020, the GDPR Standard Contractual Clauses (SCCs), an unassuming set of default contractual terms for data transfer, have drawn the attention of companies around the world. On that date, in its decision in *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* ('*Schrems II*')[1] the European Court of Justice (CJEU) abruptly redrew the landscape for exchanging personal data across borders. The CJEU struck down the EU-US Privacy Shield, the limited 'adequacy decision' that had allowed free commercial data flows between Europe and the USA under Article 45 of the GDPR. The Court upheld the validity of SCCs, the other main avenue for cross-border transfers, but set major conditions on their use.

It is difficult to understand how to meet these conditions going forward. The Schrems II Court found that SCCs were valid 'appropriate safeguards' for data transfers from EU controllers to processors outside the European Economic Area (EEA) as long as unspecified 'supplementary measures' were in place to compensate for the lack of data protection in the non-EEA country. The Court did not describe these supplementary measures, and the European Data Protection Board (EDPB)'s subsequent guidance suggests the options are quite limited.[2] Data protection officers are under intense pressure to explain these appropriate safeguards and allow routine data transfers to continue. This urgency is only increased by the context of a global pandemic requiring transfers of clinical health data to manage outbreaks and test therapeutics.

Some authorities have interpreted the decision, and the requirement for appropriate safeguards, as preventing the use of SCCs to transfer personal data outside of the EEA as private contractual safeguards can never fully redress gaps in national law. For example, the French data protection authority, CNIL, on October 9, 2020 recommended that after *Schrems II* the hosting and the management of the public 'Health Data Hub' be 'reserved for entities exclusively under the jurisdiction of the European Union;'[3] because transfer of personal data to and from such entities would not subject personal

1 Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems 2020 ECLI 559 [hereinafter Schrems II].

2 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Nov. 10, 2020) [hereinafter EDPB Guidelines].

3 Commission Nationale Informatique & Libertés, National Council of Free Software vs. Ministry of Solidarities and Health Conseil d'Etat Section du Contentieux Ref. L. 521–2 CJA (Oct. 9, 2020).

data to third country laws, unlike transfers to platforms incorporated outside the EU.[4] Following its data authority's advice, the French national health authority accordingly revised its emergency COVID-19 declaration to ban all transfers of French personal data outside the EU whether or not an SCC could be put in place.[5]

This article argues that SCCs can still be broadly useful instruments to support lawful cross-border transfers notwithstanding the CJEU ruling in *Schrems II*. SCCs currently are the dominant mechanism for cross-border transfers of personal data among commercial entities. However, limited legal scholarship exists examining the nature of SCCs. This paper traces their history and purpose within the GDPR and shows how the French supervisory authority and portions of the *Schrems II* analysis misunderstands the nature of SCCs and other Article 46 'appropriate safeguards' for transfers of personal data. Unlike country-specific adequacy rulings under Article 45 GDPR, SCCs were never intended to provide a stand-alone mechanism for transfer based solely on the adequacy of data protection law in the receiving country. SCCs, and other Article 46 'appropriate safeguards', such as Binding Corporate Rules (BCRs), provide an *alternative*, multi-layered standard for data protection that uses law, technology and organizational commitments to create an appropriate environment for an international data transfer. We argue that their purpose is to be used in situations where law alone, whether private and contractual or public and general, would be insufficient to protect data subject rights. The provisions of the SCCs themselves point to outside mechanisms, not dependent on judicial remedies, that, when combined with third-party beneficiary contractual rights within the EU, can be sufficient to safeguard fundamental privacy interests. While not perfect, the SCC's standard clauses can provide the appropriate safeguards sought by the EU. This is especially true in highly regulated contexts such as clinical trials and public health research.

The European Commission just released new draft clauses updated to reflect the passage of the GDPR in 2016 (the 'SCC's 2.0') that adopt the risk-based approach advocated here.[6] Building on the combination of law, technology and organizational commitments in the earlier transfer SCCs, the EC sets out a suite of tools, consisting of detailed impact assessments, default contractual promises and Article 32 technical security safeguards, to safeguard data subject rights even in the absence of full protection under the law of the importer. These new draft SCC clauses from the EC are helpful first steps in defining the scope of appropriate safeguards after *Schrems II*. They also illuminate the likely future of cross-border data protection governance. Entities subject to divergent legal landscapes must rely on overlapping and intersecting legal, organizational and technical standards to provide an adequate level of protection to data subjects. Where legal systems cannot converge, technology and organizational practice can. Third-party certifications and industry specific laws and codes of conduct

4 The GDPR applies to all countries in the EEA (ie including Norway, Iceland, and Lichtenstein), so it is not clear why CNIL focused solely on EU countries.

5 Arrêté du Oct. 9, 2020 modifiant l'arrêté du juillet 10, 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de covid-19 [Announcement of Oct. 9 modifying the declaration of July 10, 2020 proscribing general measures necessary to address the epidemic of Covid-19] Journal Officiel De La République Française [JO] p. 143 (Oct. 10, 2020).

6 Draft 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 (Nov. 12, 2020) [hereinafter SCC 2.0].

lower the cost of compliance and provide necessary standardization. This is especially important in the healthcare context.

II. THE LEGAL STANDARD TO TRANSFER PERSONAL DATA OUTSIDE THE EU/EEA

II.A. The Need for Global Transfers of Health Data

At the time of writing, 51 trials for a vaccine for COVID-19 are being carried out across the globe.[7] These trials require the collection and analysis of patient data in multiple jurisdictions. Patient participants must be representative of likely vaccine recipient populations, including across ethnic, gender and age lines. Efficacy must be tested in jurisdictions with active community spread. Side effects and symptoms must be monitored locally in real time. Resulting data must be transmitted back to trial sponsors and shared with public health agencies around the globe. Sponsors may subcontract to multinational cloud storage providers, genetic sequencing specialists and other private contractors. The entire effort is made up of constant, multi-layered, cross-border data flows.

The COVID-19 vaccine effort is just one example of the transnational nature of health research and patient care. Exchanges of patient and population health-related data between regions is vital for continued innovation in treatments and public health. Everything from genomic research to adverse drug reaction testing to epidemiology depends on the collection, linkage and analysis of diverse patient indicators and disease features. Research studies, including clinical trials, aim for international scope, with results being compared and matched to achieve greater statistical significance.[8] Genomics researchers worldwide rely on vast data sets gathered by consortia spanning many countries.[9] Advances in personalized medicine and use of algorithms in diagnosis and treatment depend on the analysis of massive amounts of individual statistics. These include information about risk factors, disease outcomes, lifestyle, genetics, environment, behavior, and treatment responses.[10] Makers of medical devices or academic researchers may need to store patient data with cloud service providers whose servers are located in a different jurisdiction.[11] Huge collections of health-related data are shared continuously among commercial organizations, governments, and govern-

7 Jeff Craven, Covid-19 *Vaccine tracker, Regulatory Focus* https://www.raps.org/news-and-articles/news-articles/2020/3/covid-19-vaccine-tracker (accessed Oct. 22, 2020).

8 See, eg Timo Minssen *et al.*, *The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR*, 4 Eur. Pharmaceutical L. Rev. 34, 36 (2020) (noting that multi-site trials is a necessity in many clinical trials); Maria Angeles Martinez-Grau & Maria Alvim-Gaston, *Powered by Open Innovation: Opportunities and Challenges in the Pharma Sector*, 33 Pharmaceutical Medicine 193, 196 (2019) (describing Eli Lilly's biological compound library program under which it makes its privileged compounds available to scientific institutions for testing and validation); Mark Phillips et al., *Comment: Genomics: data sharing needs an international code of conduct*, 578 Nature 31, 31 (Feb. 6, 2020) (describing large-scale cancer genomics collaboration which combined data from 468 institutions in 34 countries).

9 Philips, *supra* note 8, at 31.

10 *See* K.S. Cheung *et al.*, *Big data in gastrointestinal research*, 25 World J. of Gastroenterology 2990, 2991, 2992, 2999 (June 28, 2019); *see also* Timo Minssen et al., *Clinical trial data transparency and GDPR compliance: Implications for data sharing and open innovation*, Science & Public Policy 1 (March 2020).

11 *Cf*. Phillips et al., *supra* note 8, at 31–32 (discussing the use of cloud computing services in a large-scale cancer genomics study).

ment actors such as public health bodies, universities, and research laboratories, with significant benefits for science and global health.

II.B. The Risks of Cross-Border Transfers

Cross-border transfers of data, especially sensitive data such as that concerning health, also bring risks. The EU has enshrined privacy, protection of personal communications, and control over personal data as core fundamental rights in its Charter of Fundamental Rights.[12] Many other areas of the world do not protect privacy and personal information in the same way. Since at least 1995, the EU has restricted transfers of personal data as a way to ensure that fundamental rights guaranteed by the Charter cannot be undermined through transferring such data to less-regulated jurisdictions.[13] These protections are not limited to EU citizens. The GDPR defines 'data subjects' as any natural person whose data are processed as part of an activity regulated by EU law.[14]

The risks posed by unregulated transfers are both substantive and procedural. First, societal values of security and autonomy advanced by data protection law will be undermined if personal data are transferred for purposes that are illegal or against public policy or if the overall standard of protection is lowered.[15] Government and public authorities may function less effectively if the data they process can be accessed and analyzed by foreign entities.[16] Commercial entities may suffer if their sensitive customer and competitive data are not secure.[17] In a procedural sense, transfers to less secure jurisdictions may undermine the ability of individuals and governments to enforce protected rights.

II.C. Mechanisms in the GDPR to Mitigate the Risks of Cross-Border Transfers

To protect against these risks, Article 44 GDPR forbids transfers of personal data outside the European Economic Area except in limited, defined circumstances.[18] These restrictions ensure that the protections guaranteed by GDPR are not undermined by moving data to more permissive jurisdictions.[19] However, advances in technology have made cross-border movement of data a regular feature of many ordinary activities, such as online shopping or interactions with social media. Arguably, a 'transfer' under the GDPR can even occur if the data are accessed by a separate organization outside the EEA even if the data itself remains on servers within the territory.[20] As set out in Recital

12 Charter of Fundamental Rights of the European Union (2000/C 364/01) §§ 7, 8. [hereinafter Charter].

13 Council Directive 95/46, art. 25, 1995 O.J. (L 281) 31, 56–57 (EC) [hereinafter Directive 95/46].

14 GDPR Art. 1,2, 4 & Recital 14 ('The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data').

15 Christopher Kuner, Transborder Data Flows and Data Privacy Law 103–04 (2013).

16 *Id.* at 103–04.

17 *Id.* at 104.

18 GDPR Art 44.

19 GDPR Rec. 101.

20 Information Commissioner's Office (UK), International Transfers, Guide to the General Data Protection Regulation, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/ ('Putting personal data on to a website will often result in a restricted transfer. The restricted transfer takes place when someone outside the EEA accesses that personal data via the website.") (last accessed Nov. 17, 2020); Lexis Nexis, Practice Note: International Transfers of Data Under the GDPR 5 (last accessed Mar. 17, 2020); *but see* Criminal Proceedings against Bodil Lindqvist (C-101/01) (European Court of Justice, Nov. 6, 2003). Some wonder if *Lindqvist*'s

6 of the GDPR, 'Rapid technological developments and globalization have brought new challenges for the protection of personal data . . . Natural persons increasingly make personal information available publicly and globally. Technology ... should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organizations, while ensuring a high level of the protection of personal data'.

That said, Article 44 restrictions on transfer are not the only, or even the primary mechanism, through which this high level of protection is guaranteed beyond European borders. Through Article 2 (material scope), 3 (territorial scope) and 5 (core principles) the General Data Protection Regulation has a vast extraterritorial effect. Most notably, through the principle of 'accountability', articulated in Article 5 GDPR, the GDPR requires controllers (the entities who direct the purposes and means of data collection) to ensure adherence to core privacy principles, no matter where the geographical location of the data processing occurs.[21] Controllers may retain 'processors' to carry out specific tasks or operations in relation to data, but processors can only perform such activities according to the documented instructions of the controller and must guarantee via contract to observe and maintain the requirements of the GDPR.[22] In this way, data protection law cannot be undermined through use of 'data havens' or outsourcing in the same way that territorial environmental, labor or tax regulations famously can;[23] GDPR obligations attach to the entity controlling a particular use of personal data and follow that activity, regardless of locale or identity.

Articles 2 and 3 further define the GDPR's considerable extra-territorial reach. Articles 2 and 3 set out the material and territorial scope of the GDPR. These provisions clarify that the regulation reaches all activities of EU entities, and most processing of EU nationals' data wherever they occur. Article 2 defines processing of personal data to include all routine and/or automated processing of data other than that undertaken purely for household purposes or under limited national security or law enforcement contexts.[24] Article 3(1) states that the GDPR rules apply 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'.[25] In other words, any processing of personal data, other than the limited categories exempted in Article 2, undertaken (i) by an entity with continuous activities in the EU and (ii) that is inextricably linked with those activities must comply fully with the GDPR.[26] This is the case regardless of the location of the processing or whether

distinction between a transfer and "mere accessibility" is tenable given risks to data subject rights from making data accessible. Colin Mitchell, Johan Ordish, Emma Johnson, Tanya Brigden and Alison Hall, The GDPR and genomic data: The impact of the GDPR and DPA 2018 on genomic healthcare and research, PHG Foundation 106 (May 2020).

21 GDPR Art. 5(2); Kuner, *supra* note 15, at 72.

22 GDPR Art. 28(1), (3) & Rec. 81; EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR 3–4 https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (adopted Sep. 2, 2020).

23 Kuner, *supra* note 15, at 72.

24 GDPR Art 2.

25 GDPR Art. 3(1).

26 EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) 6–11 (Nov. 12, 2019) available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_afte

the relevant personal data relates to EU subjects.[27] In addition, Article 3(2) reaches activities of controllers and processors not established in the EU if they (a) offer goods and services to EU data subjects or if they (b) monitor the behavior of EU data subjects.[28] For example, the European Data Protection Board (EDPB) ruled in 2009 under the predecessor law to the GDPR that EU law applies directly when an EU individual enters data into an online search engine, or social network, operated from a server in another region. The EDPB took the view that in these situations, personal data are obviously flowing from the EU to third countries.[29] Similarly, a drug company using personal data to test therapeutics or medical devices for sale in the EU would fall within the ambit of Article 3(2)(a).[30] A social media or consumer wearable company collecting real-time EU subject data would be 'monitor[ing] behavior' under Article 3(2)(b).[31] The drafters of the GDPR anticipated that EU subject data and EU entities would be involved in data activities outside of EU territorial borders and took steps to comprehensively and directly regulate that processing.

In view of Articles 2, 3, and 5, the practical risks of misuse of personal data do not increase materially outside the borders of the EEA. An EU controller, operating anywhere, will face steep penalties if it entrusts the data to an unstable or fly-by-night partner, or fails to use appropriate technical and organizational safeguards.[32] The GDPR's Articles 25 and 32 require entities processing data to anticipate any risks and to incorporate protective measures by default and by design.[33] Multinationals such as Amazon, Google, or Microsoft must follow the same technical protocols wherever they engage in processing activities regulated by the GDPR. From retailers, to banks to internet service providers, companies have adapted to the mandates of the EU regulation. Those that do not face the prospect of significant sanctions. For example, the UK's Information Commissioner's Office recently fined British Airways over $25 million for failing to prevent a cyberattack that allowed hackers operating outside of the EU to embed malicious code on its booking website and siphon away consumer payment data.[34] The incentives for major private firms to adhere to the GDPR do not decrease depending on where their servers are located or in what jurisdiction they happen to access the data.[35] The material scope provisions of Article 3 already operate to encourage a standard level of protection from individual firms in any jurisdiction.

If firm-specific rules and incentives do not change outside EU borders, why then does the GDPR in Chapter 5 (containing Articles 44–50) impose additional conditions when transferring personal data to third countries? The transfer restrictions originated

r_public_consultation_en_1.pdf (stating that the notion of establishment extends to any real and effective activity—even a minimal one—exercised through stable arrangements.)

27 GDPR Art 3(1) & Recital 14 ("The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.").

28 GDPR Art 3(2).

29 *See* Article 29 Working Party, Opinion 5/2009 on online social networking (WP 163, June 12, 2009) at 5–7.

30 *See* EPBD Guidelines 3/2018 *supra* note 26, at 15–18.

31 *Id.* at [21] Example 20.

32 *eg* GDPR Art. 24, 25, 28, 32.

33 *Id.* at Recital 78.

34 ICO Penalty Notice, (Oct. 16, 2020) https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf.

35 *Cf*. EDPG Guidelines 3/2018, *supra* note 26, at 7–10, examples 1,2,4 & 5.

in the predecessor European Data Protection Directive (the '95 Directive'), which had a more limited territorial reach.[36] It is possible drafters retained the restrictions without considering fully the overlap with the new GDPR's expanded scope. Or perhaps the purpose of Articles 44–50 was to regulate the limited number of transfers that fall outside the direct reach of Articles 2, 3, and 5 of the GDPR, such as a transfer between one controller to another, unrelated controller operating outside the EU. However, only a controller located outside the EEA using historical non-sensitive EU personal data for activities that do not surveil or target EU subjects or the EU market could escape direct regulation by the GDPR.[37] The potential risks of such activities to the fundamental rights of EU subjects would seem, at present, not grave.

There is one important function for the international transfer limitations in Chapter 5 notwithstanding the GDPR's long extra-territorial reach. This purpose is to counteract risks posed by insufficient or contradictory law in a third country. A third country's law might change the ability to enforce the provisions of the GDPR in primarily two circumstances. First, local law may undermine the ability of data subjects or data protection authorities to enforce rights in third countries. Second, the positive law of third countries may impose obligations on controllers and processors that are inconsistent with the GDPR.[38] Understanding the targeted role of the transfer restrictions in the GDPR illuminates both the nature of the avenues for transfer provided in Chapter 5, including SCCs, and, as explained more fully below, the extent to which the drafters of the GDPR were willing to allow for some legal risk in the interest of beneficial transfers.

II.D. The Available Avenues for Transfer

Chapter 5 of the GDPR offers three basic pathways for a legal international transfer of data. These include:

1. transfers on the basis of an 'adequacy decision' by the European Commission (EC);[39]

36 Directive 95/46 § 4(1).

37 If the two controllers were deciding together the means and purposes of processing, as in a collaborative research project or clinical trial, then the GDPR would regulate the activities of both so long as one of the controllers was located "in the Union" (in this context the EEA). If the non-EU controller was using the data in the context of offering goods or services to EU subjects or collecting real-time EU subject data, that activity would also fall within the ambit of Article 3(2)(a) or "monitor[ing] behavior" under Article 3(2)(b). If the EU personal data qualified as sensitive 'special category data', GDPR Article 9 would apply. Article 9 allows processing, including transfers, only for narrow, limited purposes and requires suitable and specific measures under EU law to safeguard the fundamental rights and the interests of the data subject.

38 *Cf*. GDPR Recital 116 ("When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints . . . .").

39 GDPR Art 45.

2. transfers subject to 'appropriate safeguards' by the controller/processor on condition that enforceable data subject rights and effective legal remedies for data subjects are available;[40] and
3. derogations for specific situations.[41]

In effect, these mechanisms are intended to ensure an appropriate level of data protection to the data subject is provided either by: (i) the country via an adequacy decision; or (ii) the organization via adopting appropriate safeguards backed by standard contract clauses ('SCCs'), binding corporate rules ('BCRs') or codes of conduct or certifications. If none of these routes are available, the only way to transfer data is via an explicit derogation under Article 49 or to render the data anonymous so that the rules of the GDPR no longer apply.[42]

The various avenues for legal transfers in Chapter 5 are intended to ensure 'the continuity of that high level of protection' where personal data are transferred to a third country, regardless of the specific transfer mechanism employed.[43] However, each of the avenues for transfer rests on a distinct legal basis and provides continuity of protection through different means. Article 45 adequacy determinations allow transfers to jurisdictions where a government has secured a formal acknowledgement under the GDPR that their country has 'essentially equivalent' legal protections for data subjects. In the typology of transborder regulation, this is known as a geographically based 'adequacy' protection.[44]

Article 46 safeguards such as SCCs, by contrast, are organization-based approaches that rest on accountability of the controller.[45] 'Accountability' approaches require an entity regulated under host country law to compensate, through legal, technical and organizational means, for gaps in third country law. In addition to SCCs, other accountability-based mechanisms listed in Article 46 are Binding Corporate Rules ('BCRs') for transfers within related companies, and adherence to pre-approved Codes of Conduct or Certification mechanisms.

The meaning of 'accountability' in such contexts is not entirely settled. Data controllers may understand it as a way of giving them greater control over how they structure their compliance responsibilities and reduce bureaucratic burdens.[46] In this reading, it is for controllers to decide in the first instance what safeguards are 'appropriate' in a given context to protect the rights and freedoms of data subjects. Regulators, by contrast, may view 'accountability' as a mechanism for ensuring that the original data controller remains responsible for the processing activities after data are transferred.[47] Article 5(2) GDPR supports this latter position by mandating that the controller remains responsible and liable for ensuring processing in compliance with the GDPR's principles. Article 24 sets out in detail what the controller's responsibility encompasses.

40 GDPR Art. 46.
41 GDPR Art. 49.
42 GDPR recital 26.
43 Schrems II, at ¶ 93.
44 Kuner, *supra* note 15, at 64–68.
45 *Id.* at [66].
46 *Id.* at [74].
47 *Id.* at 74.

The controller must 'consider the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons', and then 'implement appropriate technical and organizational measures' to ensure adherence the GDPR.[48]

Article 49 derogations allow for limited transfers where the public interest is high, notwithstanding the lack of adequate safeguards in the third country. The EDPB has emphasized that Article 49 derogations must be interpreted restrictively.[49] Unlike Article 45 adequacy and Article 46 safeguards, Article 49 derogations fail to ensure any kind of protection of the personal data once the data has been exported outside the EEA.[50] This means that an importer could further process the data in any way permitted by their domestic laws, and even export it on additional countries without regard to the GDPR's transfer restrictions.

SCCs are the most commonly used of the Article 46 organizational 'appropriate safeguards' and arguably are the dominant mechanism for commercial transborder transfers globally. SCCs allow the transfer of personal data outside of the EU to a company that accepts the terms of standard form clauses previously approved by the EC.[51] To date three set of clauses have been approved: two between an EU controller and a controller in a third country, and one between an EU controller and a non-EU processor.[52] Each of these versions requires the data importer's agreement to the data protection law of the exporter in processing the data, to name data subjects as third party beneficiaries under the contract, and to agree to answer for breaches in a court of a member state. These clauses must be used exactly in the approved form unless an amendment is approved in advance by a data protection authority. The SCCs have been widely embraced because, at least before the *Schrems II* decision, they were viewed as the only 'off-the-shelf' data transfer solution that could be used and implemented on short notice between unrelated entities.[53]

Other off-the-shelf solutions exist in theory, such as adherence to approved Codes of Conduct or Certification mechanisms. However, the EC has not yet approved any Codes of Conduct or Certification mechanisms. This gap leaves SCCs as the only pre-approved option available in fact.

Chapter 5's narrow pathways for legitimate transfers are arguably superfluous because, as noted above, in many circumstances EU law already applies directly to all activities and parties related to the transfer. In practice, many companies have adopted Article 46 appropriate safeguards, such as SCCs, or have joined Article 45 adequacy mechanisms, such as the EU-US Privacy Shield, even though EU law already applied

48 GDPR Art. 24.

49 Commission Staff Working Document on the implementation of the Commission decisions on standard contractual clauses for the transfer of personal data to third countries (2001/497/EC and 2002/16/EC) SEC (2006) 95 p. 2.

50 *Id.*

51 GDPR Art. 46(2)(d).

52 Commission Decision 2010/87/EU 2010 O.J. (L39) 5 [hereinafter 2010 Clauses]; Commission Decision 2001/497/EC 2002 OJ (L6) 52 [hereinafter 2001 Clauses] *modified by* Commission Decision 2004/915/EC 2004 O.J. (L385) 74 [hereinafter 2004 Clauses].

53 See Lexis Nexis, *supra* note 20, at 17 (calling the SCC model clauses a "straight forward tick box solution" that is "simple and quick to execute").

to them directly under Article 3 of the GDPR.[54] This 'belt and suspenders' approach is understandable as a risk mitigation procedure on an individual firm level. On a regulatory level, however, commentators have noted that it seems incoherent to require two overlapping sets of rules that are not coordinated with each other simultaneously to regulate transborder data flows.[55] The lack of a unitary framework between the scope and transfer provisions creates confusion and increases compliance costs unnecessarily. Even in circumstances where additional protections are useful, such as where local law conflicts with EU law, Articles 45 and 46 offer little guidance about how such conflicts should be resolved.

II.E. The Schrems II Decision

The *Schrems II* case was a missed opportunity to clarify how to transfer data safely using 'accountability' when local and EU law conflict. Instead, the court repudiated or made unstable the two principal mechanisms for data transfers to the USA. The end result is to reduce the available channels for transferring personal data from the EU to third countries. The ruling tightened the meaning of 'adequacy' under Article 45. It also seemed to define accountability under Article 46 so broadly as to include responsibility for ensuring the adequacy of third country law. Such a broad ruling threatens to have Article 45's adequacy test swallow the rest of the transfer mechanisms. Indeed, some regulators have interpreted the *Schrems II* decision as essentially banning transfers to the USA or US entities under any circumstances.

The *Schrems II* decision is the latest chapter in a multi-year saga concerning objections by an Austrian national, Maximilian Schrems, to the transfer of his personal data from Facebook Ireland to its US parent Facebook Inc. for processing. Schrems contended that US law requires Facebook Inc. to make the personal data transferred to it available in bulk to certain US authorities, such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) for national security monitoring.[56] He submitted that these blanket monitoring programs conflicted with Articles 7, 8, and 47 of the EU Charter, rendering it impossible for Facebook Inc. to comply with both US and EU law. In those circumstances, Mr Schrems asked the Commissioner to prohibit or suspend the transfer of his personal data. Schrems submitted that the SCCs in effect between Facebook Ireland and Facebook Inc. did not limit US authorities and so could not justify the transfer of that data to the US under Article 46.[57] He also sought a ruling from the Irish data protection authority that the limited Article 45 adequacy finding for the USA, the EU-US Privacy Shield, was in error.

The CJEU agreed with Schrems and struck down the EU-US Privacy Shield.[58] The court determined that SCCs could still be used to transfer data to jurisdictions without an adequacy ruling such as the USA as long as 'essentially equivalent' protections for EU

54 See Christopher Kuner, *Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law*, 5 Int'l Data Privacy Law 235, 244 (2015).

55 *Id.* at 244.

56 Schrems II, at ¶ 55.

57 Schrems II ¶¶ 151–153.

58 Schrems II ¶ 201.

personal data could be assured.[59] The ramifications of the decision have sent privacy lawyers and regulators scrambling to determine how legally to continue data flows between the EU and much of the rest of the world.

The *Schrems II* decision is odd in several respects. First, with respect to Article 45 adequacy, the CJEU had many valid grounds through which to find the Privacy Shield inadequate, but national security was perhaps the weakest and most problematic. Second, the decision destabilized the use of Article 46 'appropriate safeguards' as pathways to transfers as well. Instead of treating the question of organizational safeguards as a separate and distinct legal inquiry, the CJEU appears to have collapsed the legal adequacy pathway of Article 45 and the appropriate safeguards test of Article 46 together. That result would shrink all of Chapter 5's avenues for transfer into one adequacy test that is functionally unattainable.

The Privacy Shield, a *sui generis* agreement negotiated by the EC with the US government, is problematic under both EU and US law.[60] As a voluntary program, the Shield lacked the force of generally applicable law. The framework permitted data transfers to companies that self-certify adherence to GDPR-like rules. The purpose of an adequacy inquiry under Article 45 is to examine whether a third country's legal framework is sufficiently protective, so the Privacy Shield would seem to fall at the first hurdle.[61] The Privacy Shield also failed to meet Article 46 standards for voluntary mechanisms like codes of conduct or certifications, which it more closely resembled.[62] The U.S. Department of Commerce and the Federal Trade Commission pledged to enforce its terms but the EU Commission persistently faulted the agencies for failing pro-actively to audit participating entities.[63] Many organizations, such as Facebook, claimed to comply but in fact continued to use personal data for illegitimate purposes in violation of GDPR rules. At the same time, the Privacy Shield as understood by the EC was incompatible with US law because, it required federal agencies to conduct protective audits for the sole benefit of EU citizens, activities arguably outside the agencies' powers.[64] All of these flaws would have been valid grounds for finding the Privacy Shield invalid under Article 45.

Instead the *Schrems II* complaint, and the CJEU decision, looked at US government access to personal data for national security purposes, and whether EU citizens had

59 Schrems II ¶ 203(b) ("Article 46(1) and Article 46(2)(c) of Regulation 2016/679 must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter of Fundamental Rights of the European Union.").

60 Laura Bradford, Mateo Aboy and Kathleen Liddell, *International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an 'adequate' level of protection'* J. L. AND THE BIOSCIENCES, 1, 12 (2020).

61 *See, eg* Court of Justice of the European Union Press Release No 165/19, Advocate General's Opinion in Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Luxembourg, Dec. 19, 2019).

62 Bradford et al, *supra* note 60, at 14.

63 Commission Staff Working Document Accompanying the document, Report From the Commission To The European Parliament and The Council on the third annual review of the functioning of the EU-U.S. Privacy Shield 25–27 COM(2019) 495 final (23 Oct., 2019).

64 Bradford et al., *supra* note 60 at 17.

the same rights of judicial review and redress available to them in the EU.[65] Under EU law, including the GDPR, any access to personal data for national security purposes that trespasses on privacy rights must be 'necessary and proportionate'.[66] At the same time, national security policy is the sole responsibility of the Member States. In effect, each EU Member State is given discretion to balance national security needs with data privacy rights.[67] Yet, the CJEU ruled in *Schrems II* that third countries such as the USA were not entitled to similar discretion.[68] The court then went on to find that the US approach to national security monitoring was not necessary and proportionate.[69] Meanwhile, when asked to consider similar EU legislation in a subsequent case, the CJEU adopted a more deferential posture. It allowed Member States to authorize indiscriminate collection and retention of sensitive data from service providers for national security purposes when 'facing a serious threat to national security'.[70] Although such retention authority should be 'limited in time to strictly necessary', subject to safeguards and conditions and 'not systematic in nature', it may be renewed due to an 'ongoing nature of the threat'.[71] With respect to less sensitive data such as IP addresses, the Court permitted general and indiscriminate retention for the objective of fighting serious crime and preventing serious threats to public security.[72] Through this finger on the scale, the CJEU framed broad US programs as a special risk that EU citizens do not face at home when that is not entirely true. Of course, one could always claim that surveillance by one's own democratically elected government is preferable to surveillance by third countries. However, if every government adopted this approach to the adequacy of other countries' laws, all cross-border transfers would halt immediately.[73] An adequacy standard that allows the CJEU to interrogate the national intelligence operations of non-EU countries but not Member States is an incoherent and somewhat outrageous outcome.

The *Schrems II* decision threatens the viability of the Article 45 legal adequacy test going forward. Under the GDPR, the EC determines whether a country outside the EU offers an adequate level of data protection. For the level of protection in a third country to be considered adequate, it must offer guarantees to the data subject 'essentially equivalent' to those offered in the EU.[74] The means of protection, however, may differ

65 Schrems II ¶¶ 178–200.

66 Charter Art. 52(1); GDPR Art. 23.

67 Joshua P. Meltzer, *The Court of Justice of the European Union in Schrems II: The Impact of the GDPR on data flows and national security, Brookings Report* Aug. 5, 2020, https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/ (last accessed Sep. 24, 2020).

68 Schrems II ¶ 81.

69 *Id.* at ¶¶ 178–200.

70 C-623-17, Privacy International 2020 ECLI 790, C-511/18, La Quadrature du Net and others, 2020 ECLI 791.

71 Quadrature du Net and others ¶¶ 136–39.

72 *Id.* at ¶¶ 152–59.

73 *Cf*. Anupam Chander, *Is Data Localization A Solution for Schrems II*, forthcoming J. Int'l Econ. L., at 11 (draft, July 27, 2020) (noting that other countries that have adopted GDPR-like laws may demand that the EU stop surveilling their citizens).

74 GDPR rec. 104; Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650,191 ¶ 73 (Oct. 6, 2015) [hereinafter Schrems I] (holding that "while the term 'adequate' cannot require a third country to ensure a level of protection identical to that guaranteed in the EU legal order, . . . [it still] must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments,

from that in the EU, so long as they prove as effective in practice.[75] When assessing whether a third country's law and practice are adequate under the GDPR, the EC has also taken into account the significance of a trading partner, both commercially and in terms of cultural ties to the EU, and strategic objectives in continuing important data flows and encouraging legal reform.[76] In other words, the EC has weighed the benefits of continued data flows as well as risks in determining 'adequacy'.[77] To date, the EC has recognized 12 countries as providing adequate protection: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay.[78]

The CJEU, by contrast, in considering challenges to adequacy determinations, considers only whether the third country provides privacy protections consistent with the Charter of Fundamental Rights of the EU. In *Schrems II*, the Court conducted a detailed analysis of specific provisions of US national security laws and found those laws to lack the required 'clear and precise rules governing the scope and application . . . and imposing minimum safeguards'.[79] This approach changes the scope of an adequacy inquiry from one of general effectiveness, to specific, fine-grained equivalency. This approach undermines other existing Article 45 adequacy rulings as it is unlikely that Israel, for example, or Argentina or Japan could meet *Schrems II*'s new equivalency threshold for law enforcement surveillance.[80] Going forward, the focus of the CJEU in *Schrems II* on consistency with the EU Charter for Article 45 adequacy leaves little room for different approaches to privacy in other countries and narrows the scope for Article 45 adequacy findings generally.[81]

The *Schrems II* ruling undermined the use of Article 46 'appropriate safeguards' as well. In the absence of an adequacy decision, Article 46(1) of the GDPR allows appropriate safeguards to be taken by the controller or processor that 'compensate for the lack of data protection in a third country'.[82] One could read the word 'compensate' in Recital 108 to mean alternative technical means, or via legal remedies available in the host country. The CJEU read it narrowly, however, to mean capable of ensuring 'a level of protection essentially equivalent to that which is guaranteed within the European Union', ie specific legal adequacy as under Article 45.[83] The basis for this obligation is

a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter [of Fundamental Rights of the European Union].").

75 Schrems I, *supra* note, at 75, at ¶ 74; *Article 29 Data Protection Working Party, Adequacy Referential* (updated), WP 254, at 2 (Feb. 6, 2018) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

76 European Commission Memo/17/15, Digital Single Market—Communication on Exchanging and Protecting Personal Data in a Globalized World Questions and Answers, (Jan. 10, 2017) http://europa.eu/rapid/press-release_MEMO-17-15_en.htm.

77 Paul Roth, *Adequate level of data protection' in third countries post-Schrems and under the General Data Protection Regulation*, 25 J.L. Inf. & Sci. 49, 60–1 (2017); Jennifer Stoddart, Benny Chan, and Yann Joly, *The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research* 44 J. Law Med. Ethics, 143, 147–49 (2016).

78 European Commission, Adequacy Decisions, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last accessed Nov. 22, 2020).

79 Schrems II ¶ 180, 184.

80 Meltzer, *supra* note 61.

81 *Id.*

82 GDPR recital 108.

83 Schrems II ¶ 96.

not completely clear. At times, the Court suggests that the EU Charter itself requires this standard.[84] In other places the Court cites specific clauses of the SCCs requiring the Parties to warrant full compliance with the GDPR as the source of the equivalency obligation.[85]

The CJEU held that SCCs remain viable where the controller adduces 'supplementary measures' to rectify legal flaws that would otherwise undermine equivalency.[86] The Court provided little guidance about what kinds of measures might be effective in this regard. The problem with SCCs (and BCRs and Certification mechanisms etc.) is that they are contractual mechanisms between private parties that do not bind other governments. Therefore, where third country law or practice is inconsistent with the GDPR, SCCs cannot remedy that problem. Indeed, the Court went on to say that data controllers, and Data Protection Authorities, must suspend transfers to any jurisdiction where it finds that 'an obligation [allowing processing of personal data] prescribed by the law of the third country of destination . . . goes beyond what is necessary' and so conflicts with the GDPR.[87]

Read broadly, the decision could forbid any transfer, whether under Article 45, 46, or another provision of Chapter 5, unless the legal rights of EU citizens in third countries would be specifically equivalent to those available under EU law. Rather than treating Article 45 and Article 46 as separate pathways, the *Schrems II* analysis seems to collapse all of Chapter 5 into a narrow legal adequacy determination. However, unlike Article 45 adequacy, which must be determined by the EC and the European Data Protection Board after a detailed investigation, Article 46 legal adequacy must be evaluated by individual controllers in the first instance.[88] The question of whether the regulations of a third country allow processing 'beyond what is necessary' when compared to the EU is not a simple one. It is also unclear what kind of contractual supplementary measures (if any) could counteract a mandatory law or provide a judicial remedy against the government where such remedy does not already exist. A wrong guess may leave controllers and processors liable to the full range Article 83(5)'s penalties, including fines of up to €20 million or 4 per cent of worldwide annual turnover.[89] The Court did leave open the possibility of transfers in the specific circumstances justifying an Article 49 derogation, such as necessary for performance of a contract, but it is unclear on what basis the Court considers that EU fundamental rights are justifiably compromised in these circumstances.[90] Given how narrowly the Court defined adequacy, arguably no

84 Schrems II ¶¶ 99–101.

85 Schrems II ¶¶ 140–142 (citing 2010 SCCs ¶¶4(a), 5(a)&(b)).

86 Schrems II ¶ 103, 134.

87 Schrems II ¶¶ 141–42.

88 Schrems II ¶¶ 134, 142 ("It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses . . . . It follows that a controller established in the European Union and the recipient of personal data are required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned. The recipient is, where appropriate, under an obligation, under Clause 5(b), to inform the controller of any inability to comply with those clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract.").

89 GDPR ¶ 83(5).

90 Schrems II ¶ 202.

transfers to jurisdictions with active national security data collection, such as the USA, can ever occur.

Some EU regulators have drawn exactly this conclusion. On October 10, 2020, the French Ministry for Health and Solidarity made an emergency change to its Covid-19 law to forbid the sharing of French public health data outside of the European Union. The change was in response to an action brought by the French National Commission for Informatics and Freedoms (CNIL), the French data protection authority, requesting that data from the French national public health registry no longer be entrusted to servers run by the Microsoft Corp., or any of its subsidiaries, because those companies were subject to US national security laws.[91] CNIL dismissed the use of Article 46 SCCs and supplementary measures as a corrective because such measures could never prevent direct access by US intelligence.[92] The Conseil d'Etat, the highest French administrative court, agreed that after *Schrems II*, no personal data transfer to the USA would be possible under either Article 45 or 46.[93] However, the Court was willing to allow Microsoft's Irish subsidiary to continue hosting and processing data in the EU on one condition. The Court required Microsoft to amend its contract to state that it would follow only the law of the EU, and not the USA, with respect to granting access to public authorities. In other words, in the event of a conflict, Microsoft must choose EU law.

Other Data Protection Authorities (DPAs) have not gone quite so far, but still have narrowed the range for permissible transfers. The DPA for German State of Baden-Württemberg is so far the first and only member state DPA to provide official guidance on transfers in the wake of *Schrems II*.[94] The guidance requires controllers first to determine whether the cross-border transfer is necessary, or whether another solution, such as processing the data within the EU, is available.[95] The guidance allows use of Article 46 mechanisms, such as SCCs and BCRs, alongside 'supplementary measures' to protect the data if transfer to the third country cannot be avoided, and the controller determines that the legal protections in the third country are sufficiently adequate. In light of the decision in *Schrems II*, it is difficult to see how a controller could determine the legal protections in the USA are sufficiently adequate. The European Data Protection Supervisor, the regulator responsible for ensuring the compliance of EU agencies with the GDPR, similarly 'strongly encourage[d]' its agencies to avoid any processing activities that involve transfers of personal data to the US.[96]

The EDPB's recently issued Guidelines (EDPB Guidelines) adopt the CJEU's restrictive reading of adequacy. The EDPB Guidelines require those who rely on Article 46 safeguards to guarantee an equivalent level of protection in the third country, if

91 Commission Nationale Informatique & Libertés, *supra* note 3, at 5.

92 *Id.* at [5].

93 Arrete du Oct. 9, *supra* note 5 at 143.

94 Omar Malik & Maria Khan, *Understanding Baden Wurttemberg's Updated Guidance on International Data Transfers* IAPP.org, (Sep. 24, 2020) https://iapp.org/news/a/post-schrems-ii-understanding-baden-wurttembergs-updated-guidance-on-international-data-transfers/.

95 *Id.*

96 European Data Protection Supervisor, *Strategy for Union institutions, offices, bodies and agencies to comply with the Schrems II Ruling*, Oct. 29, 2020 https://edps.europa.eu/sites/edp/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf.

necessary through the use of 'supplementary measures'.[97] The EDPB also does not distinguish whether this equivalency is required to protect fundamental rights under the Charter, or merely to ensure that importers do not breach their obligations under the wording of the existing SCC Clauses.[98] The Guidelines state that 'in principle, supplementary measures may have a contractual, technical or organizational nature' but that generally 'only technical measures' such as secure encryption will be effective to impede access by foreign authorities.[99] This Guidance is less restrictive than the French approach but would still preclude sharing data with any entity requiring unencrypted access to the raw data even if for the purpose of health research or drug discovery.[100]

In contrast, the EC in current SCCs and the SCCs 2.0 just released sets out a more pragmatic approach. As detailed below, the existing clauses set out a risk-based and calibrated framework for measuring legal adequacy under Article 46. The EC approach would tolerate some gaps in third country laws where data subject rights can be protected using other mechanisms.

The narrow regulatory interpretations adopted in *Schrems II* are also out of step with the market realities of data exchange. Surveys conducted after the decision among EU data controllers find that the majority (88%) do not intend to reduce their data exports to the US or to non-EEA/non-UK jurisdictions despite the risks.[101] The majority plan to use Article 46 SCCs as transfer mechanisms and to try to implement supplementary measures to counteract legal deficiencies.[102] A shared understanding of what Article 46 permits, and what kinds of 'supplementary measures' can legitimate transfers using SCCs has never been more important.

III. THE HISTORY, NATURE, AND STRUCTURE OF GDPR ARTICLE 46 AND EUROPEAN COMMISSION STANDARD CONTRACTING CLAUSES

Article 46 is already designed to mitigate for legal inadequacy through multi-layered technical and organizational measures. The current and new proposed SCCs rely on domestic law, private contractual commitments and technological measures to compensate for inadequate local law. This approach allows SCCs to continue to facilitate important data flows throughout the world, including for health research purposes.

III.A. Accountability as an Alternative to Adequacy

SCCs first appeared in the wake of the European Convention 108, the first legally binding international instrument for data protection and the 1995 EC Data Directive.[103] The Convention 108 entered into force on October 1, 1985. Its purpose was to promote cross-border transfers of data among states demonstrating a shared commitment to privacy principles by accession to the Convention. The original instrument addressed only trans-border exchanges between Convention signatories, and provided that these should not be restricted except in limited circumstances. One of the circumstances was

97 EDPB Guidelines, *supra* note 2, at ¶¶ 28–29.
98 *Id*. at ¶¶ 29–30, 34.
99 *Id*.at ¶¶ 45, 48.
100 *Id*. at Annex 2 Use Cases 6 and 7.
101 Fieldfisher, *The results are in: How Schrems II will impact international data flows in practice* (Sept. 9, 2020).
102 *Id* at Questions 4 & 6.
103 European Convention 108.

concern about further transfers to non-Party states. As economic and technological developments made such third-country transfers increasingly likely, it became necessary to set rules so that a Convention signatory could allow such transfers without risking its own access to Convention member data.[104] In 1995, the new EC Data Directive mentioned the possibility of standard contractual clauses as a method for Member States to provide adequate safeguards for cross-border transfers.[105] In 2001, the Council of Europe adopted an Additional Protocol to the Convention 108, which set out the three-pronged adequacy, derogation, or safeguards pathway for transfers outside of Convention territories.[106] These three options are preserved in Chapter 5 of the GDPR.[107]

Both the EC Data Directive of 1995 and the 2001 Additional Protocol define appropriate safeguards such as SCCs as a ***derogation from*** legal adequacy. Article 2(1) of the Protocol contains an adequacy test: it provides that transfers of personal data to a non-party state are permitted only if that state assures an 'adequate level of data protection'. Article 2(2) then provides:

> By way of derogation from paragraph 1..., each Party may allow for the transfer of personal data:
> a. if domestic law provides for it because of:—specific interests of the data subject, or.—legitimate prevailing interests, especially important public interests, or.
> b. if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.[108]

A 'derogation' is an exemption or relaxation of a rule. The Protocol defines appropriate safeguards like SCCs as an exemption from third country legal adequacy, on par with countervailing considerations such as important public or data subject interests.[109] The safeguard for Article 2(2)'s derogations is the supporting structure of domestic law, in contrast with Article 2(1)'s focus on the law of the receiving state.

The EC Data Directive 95/46 similarly lists standard contractual clauses and adequate safeguards for cross-border transfers under Article 26 as 'derogations' from the need for a full country adequacy decision under Article 25.[110] In a 1998 Working Document, the WP 29, the predecessor body to the EDPB, explored ways to make the safeguards in such clauses enforceable through reliance on the law of the state of the exporter.[111] The primary mechanisms discussed included (1) holding the EC exporter liable to the data subject for actions of the importer, (2) requiring the importer to

104 Council of Europe, Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows ¶¶ 23–24 (Nov. 8, 2001).

105 Directive 95/46 § 26(2).

106 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, July 1, 2004.

107 GDPR Art. 45–49.

108 Additional Protocol, § 2(2).

109 Directive 95/46 § 26(2).

110 Directive 95/46 § 26(2).

111 WP 29, *Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries*, DG XV D/5005/98 final 6 (adopted April 22, 1998) available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp9_en.pdf.

submit to the authority of courts and supervisory authorities in the exporter's home state.[112]

Article 46(1) of the GDPR preserves this structure of 'appropriate safeguards' offering a separate pathway for transfers to legally problematic jurisdictions based in domestic law. Article 46(1) provides:

> In the absence of a[n adequacy] decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

The requirements of Article 46 are additive. First, to make up for a lack of legal adequacy in the destination state, the controller or processor must provide 'appropriate safeguards'. Paragraph 2 goes on to give examples of such safeguards, including SCCs, BCRs and the like. Second, enforceable data subject rights and effective legal remedies must be available.

Article 46 does not specify whether those enforceable rights must stem from the law of the destination jurisdiction or whether rights enforceable under domestic law of the transferor suffice. However, enforceable rights and effective remedies are the *sine qua non* of legal adequacy determinations, and Article 46(1) is intended for situations where such adequacy may not be present in the destination country. It seems likely then that the drafters intended that rights and remedies under the originating country's domestic law would suffice. Furthermore, Article 2(2) of the Additional Protocol rooted the concept of adequate safeguards in the transferor's domestic law, and Article 46(1) is a direct descendant of that provision.

On November 12, the EC released long-awaited new proposed SCCs updated to reflect the GDPR rather than the 1995 Directive (the 'SCC 2.0'). If accepted, the SCC 2.0 would replace the current versions sometime in 2021, with a one-year transition period.[113] In its draft decision implementing the New Clauses, the EC asserts that the clauses themselves already provide enforceable rights and effective remedies. Section 1 'Purpose and Scope' of the SCC 2.0 states 'These Draft Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies pursuant to Article 46(1) and Article 46(2)(c) of [the GDPR]. .. provided they are not modified ... '.[114] This statement supports the idea that 'enforceable rights' and 'effective legal remedies' grounded in domestic law of the exporter, as set out in the clauses, are sufficient to protect data subject interests.[115]

112 *Id.* at [6–9].

113 Draft Commission Implementing Decision on SCC 2.0 ¶ 24.

114 SCC 2.0 §1

115 See also Draft Commission Implementing Decision on SCC 2.0, at ¶ 11 ("In order to provide appropriate safeguards, the standard contractual clauses should ensure that the personal data transferred on that basis are afforded a level of protection essentially equivalent to that which is guaranteed within the Union.") The EC in this passage defines ensuring effective protection as part of the essential requirements of the "appropriate safeguards' and not as a separate and supplementary legal requirement.

III.B. Enforceable Data Subject Rights and Remedies

The new and existing SCC clauses (together, the 'Clauses') have a dual nature as both private contract and public instrument granting enforceable rights to third parties under domestic law. The Clauses contain three sets of interlocking obligations for the parties to (i) abide themselves by GDPR fundamental principles (Appendix 1/Annex 1) (ii) extend enforceable rights and remedies to data subjects under the law of the exporter, (main body) and (iii) adopt technical and organizational measures, tailored to the specific risks of the transfer, to ensure security of processing (Appendix 2/Annex 2). Once the exporter chooses to transfer under the clauses, the parties are in effect opting into an additional set of default legal requirements calibrated to ensure continuous protection to data subjects.

Although the Clauses nominally are private obligations, they display many features of public law. For example, only the EC or member country DPAs can create and adopt viable clauses.[116] The three existing clauses were developed by the EC acting under the authority of the 1995 Directive. Two of the approved clauses relate to transfers between EU controllers and controllers in third countries. The first version was approved by EC decision in 2001 and the second in 2004. The third set, for use between EU controllers and non-EU processors, was approved in 2010. The SCC 2.0 proposed in 2020 cover an expanded array of processing scenarios, including EU processor to non-EU controller, and processor to sub-processor transfers. Businesses had been asking for these additional templates for years, and also to have updated terms to reflect the passage of the GDPR in 2016. However, without action by the EC, parties are powerless to devise their own rules. The SCC 2.0 finally addressed these needs. The terms of these clauses are mandatory and cannot be amended by either Party without sacrificing the safe harbor of Article 46.[117] In this respect, these default terms operate as an 'opt-in' set of legal rules.

The structure of each set of the Clauses is similar and functions primarily to create enforceable rights for data subjects under the domestic law of the exporting country. First, Section 1 of each version requires the exporter and importer set out the details of the transfer in an Appendix or Annex. In this Annex 1, the parties must consider and list the nature and category of the data involved, and the underlying purpose of the transfer. Annex 1 is, therefore, a blueprint for the parties' consideration and resolution of the GDPR's foundational principles, such as lawfulness, transparency, purpose limitation and data minimization, in relation to the specific data flow. The specificity required by Annex 1 ensures adherence to these principles by requiring affirmative steps beyond signing traditional contractual boilerplate simply to abide by governing law.

Second, the main body of Clauses contain exporter and importer promises that can be enforced by data subjects themselves. Each version requires that the exporter and importer agree that the law of one of the EU Member States governs the contract,[118] and that data subjects can invoke and enforce the clauses as third party beneficiaries for almost all of the listed obligations.[119] To ensure effective enforcement, the data

116 GDPR Art 46(2).
117 GDPR Recital 109.
118 SCC 2.0 §III ¶3; 2010 Clauses ¶ 9; 2004 Clauses §4; 2001 Clauses ¶ 10.
119 SCC 2.0 §I ¶ 2; 2010 Clauses ¶ 3; 2004 Clauses § III(b); 2001 Clauses ¶ 3.

importer must agree to submit to jurisdiction in the chosen Member State and to abide by any decisions under that country's law.[120]

Section 2 of the Clauses sets out the specific obligations of the Parties. In the 2001, 2004, and 2010 Clauses, these obligations include ensuring compliance with either the law of the exporter or the principles of the 95 Directive.[121] The 2010 controller to processor clauses add obligations for the exporter to ensure that 'the processing. .. of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law'.[122] As of May 2018, this law would be the GDPR, or its domestic equivalent. This includes ensuring the security of the data using appropriate measures.[123] The importer, for its part, promises essentially that (i) no domestic law prevents it from complying with the clauses, (ii) that it will follow the GDPR in processing the data, (iii) that it will respond promptly to requests from the data subject, exporter or supervisory authority, and (iv) to submit its premises to audit upon request.

Each version of the Clauses gives data subjects at least one entity accountable to suit in the EEA for compensation in the event of a breach of any of the third-party beneficiary rights. Where the importer is a controller, the Clauses have moved from joint and several liability under the law of the exporter (the 2001 clauses)[124] to each Party being accountable to the data subject for its own actions (the 2004 clauses) so long as the exporter used reasonable diligence in assessing the ability of the importer to comply with the contract.[125] The SCC 2.0 controller-to-controller clauses retain joint and several liability where more than one party has caused damage.[126] They also expand the obligation of the exporter to conduct reasonable diligence on the importer to every kind of transfer, whether between controllers, processors or a mix.[127]

Where the importer is a processor, the Clauses rely more explicitly on controller accountability to provide redress to data subjects. The 2010 controller to processor clauses require the exporter to remain responsible to data subjects for any breach of the clauses whether by itself or by its processor. Only in 'exceptional' cases, where the exporter has disappeared or become insolvent may the data subject bring an action directly against the importer.[128] The SCC 2.0 controller to processor and processor to sub-processor transfers are not quite so prescriptive and allow suit against either the importer, the exporter or both in the case of damage caused by the importer.[129] In this way, every version of the Clauses ensures that the data subjects will always have redress against a private entity within the EEA. The primary result, then, of the default Clauses is to create enforceable data protection rights and effective avenues of redress for data subjects in an EU Member State.

120 SCC 2.0 §II ¶6(b)(d) (except EU processor to non-EU controller modules), §III ¶ 3(a); 2010 Clauses ¶ 7; 2004 Clauses § V ¶3; 2001 Clauses ¶ 7.
121 2001 Clauses ¶ ¶ 4(a), 5(a)&(b); 2004 Clauses §§I(a), II(h); 2010 Clauses ¶¶ 4(a)&(b), 5(a).
122 2010 Clauses ¶ 4(a).
123 2010 Clauses ¶ ¶ 4(c)-(e).
124 2001 Clauses Implementing Decision ¶18.
125 2004 Clauses § I(b)&III(a)
126 SCC 2.0 ¶ 7 (controller to controller and processor to controller modules).
127 *Id.* at §II ¶1.
128 Implementing Decision 2010 Clauses ¶ 20; 2010 Clauses ¶¶ 3(10, 3(2), 6(1) & 6(2).
129 SCC 2.0 ¶ 7 (controller to processor & processor to processor modules)

Third, the Clauses build in a number of mandatory safeguards beyond strictly legal remedies. The 2010 Controller to Processor Clauses require that the Parties warrant use of appropriate, state of the art, organizational and technical measures to protect the data against accidental or unlawful intrusion.[130] The exporter must warrant specifically that the security measures are appropriate to the risks and the nature of the data being transferred.[131] The precise measures adopted must be listed in Appendix 2. Taken together with the purpose specifications in Appendix 1, the dual appendices operate as a form of diligence checklist ensuring that the parties proactively consider and list practical protective measures targeted to identified risks.[132]

The SCC 2.0 update and expand this requirement in line with Article 32 GDPR, Security of Processing, and its accompanying recitals. Article 32 requires, '[t]aking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk'. The measures identified there include pseudonymization, encryption, minimization, contractual secrecy and employment training, each suited to the purpose, means and risks of the processing.[133] The SCC 2.0 place the obligation to ensure security of processing on the importer specifically.[134] However, to the extent the GDPR applies to the activity, both parties could be directly liable for failing to implement necessary security measures.[135] Where the transfer is to a processor, 'Annex II' still requires a detailed list of the specific measures taken by the importer.

The appropriate safeguards provided by the Clauses then are three-fold. First, Annex/Appendix 1 requires the Parties to consider and demonstrate compliance with the GDPR's governing principles. Second, the clauses themselves ensure enforceable data subject rights and effective remedies under domestic law. Third the Clauses require the parties to analyze the contemplated data flow and identify technological and organizational measures that are appropriate to address specific risks. Boilerplate statements simply stating that a party complies with the requirements of the GDPR do not suffice; affirmatively-stated details are required. The result is a multi-faceted and layered approach to protection that does not depend on rights in the importing state.

III.C. SCCs and Third Country Legal Conflicts: A Risk-Based Approach

The EC implementing decisions for the existing SCCs and the SCC 2.0 also shed light on how to evaluate the sufficiency of third country law under Article 46(2), as opposed to adequacy under Article 45(3). Article 45 adequacy allows transfers to proceed with no additional safeguards. In such circumstances, the receiving legal framework alone must provide minimum and non-negotiable levels of protection. The

130 2010 Clauses ¶ 4(c)&(d).

131 2010 Clauses ¶ 4(d).

132 The controller to controller clauses do not contain specific requirements relating to technical and organisational measures. However, the threat of joint and several liability or liability for failing to conduct due diligence may operate in practice to ensure that such proactive measures are taken.

133 GDPR Art. 32.

134 SCC 2.0 § II ¶ 1.5(a) (controller to controller module); ¶ 1.6(a) (controller to processor and processor to processor modules).

135 *See, eg* GDPR Art. 24, 25 & 28.

SCC implementing decisions in 2001, 2010, and 2020 (draft) suggest that a different standard applies when the SCC clauses, with their multiple domestic protections, apply. In particular, the SCC decisions point to an important role for supervisory authorities to exercise discretion in weighing whether conflicts with third country law justify the suspension or prohibition of data flows. This more permissive stance makes sense considering (i) the broad extra-territorial reach of the GDPR and (ii) the multiple safeguards already operating within the SCCs to limit access to protected data.

1. The 2001 and 2010 SCCs and Implementing Decisions

Some inartful drafting in the 2010 Clauses contributed to the confusion in *Schrems II*. The 2010 Clauses require the exporter to warrant that all processing of the data, pre- and post- transfer, will be done in accordance with the data protection law of the EU/EEA Member State where the exporter is established (ie initially the Directive 95/46/EC and currently the GDPR).[136] This blanket guarantee, which extends beyond the actions of the parties themselves to include any entity accessing the data post-transfer, can be read to include a warranty that any government accessing data will also comply with every aspect of the GDPR. This contractual promise is the immediate source for the CJEU's insistence in *Schrems II* on equivalency between the GDPR and the importer's data protection law.[137]

The EC has made clear in its implementing decisions for the 2001 and 2010 clauses, however, that it did not intend to make strict legal equivalency a pre-condition for transfer under Article 46. Instead, the EC laid out a risk-based approach. The 2001 and 2010 SCC Decisions name the supervisory authority as the appropriate entity to weigh conflicts between legal regimes under Article 46.[138] In the event of a material conflict with foreign law, the parties must alert the relevant supervisory authority, who will then consider whether the transfer can proceed notwithstanding the conflict.[139] The Decisions then outline a deliberative process. The authority must consider (a) whether the third country legal requirements go beyond what is proportionate in a democratic society and (b) if so, whether the requirements are *likely to have a substantial adverse impact* on the guarantees provided by the member state data protection law and the SCCs.[140] In other words, the main obligation of data exporters and importers in the event of a serious legal conflict is to notify supervisory authorities.[141] It is then for the supervisory authority to evaluate whether the law irreconcilably conflicts with the GDPR (by being disproportionate to its aims) and whether that conflict is likely to have a 'substantial adverse impact' in the instant case. The supervisory authority necessarily may consider the protections inherent in the SCC itself in weighing the likelihood of a substantial adverse impact. The mere possibility of an impact would not be sufficient. For example, presumably if the data concerned is (a) not of a type likely to be of interest to national security agencies, (b) pseudonymized and (c) encrypted, a transfer might

136 2010 Clauses ¶ 4(a); see also Decision 2010 Clauses ¶ 18.

137 Schrems II ¶¶ 140–142 (citing 2010 SCCs ¶¶4(a), 5(a)&(b)).

138 Decision 2010 Clauses ¶¶ 11,18 § 4(a), Decision 2001 Clauses § 4(a).

139 2010 Clauses ¶ 4(g); 2001 Clauses ¶ 5(a).

140 Decision 2010 Clauses ¶¶ 11,18, § 4(a), Decision 2001 Clauses ¶ 15, § 4(a).

141 Exporters also have discretion to terminate the transfer themselves if they believe the legislation is likely to have a substantial adverse impact. 2010 Clauses ¶ 5(b).

still be permitted even if third country law fails to outlaw disproportionate surveillance. This framework sets out a permissive structure wherein transfers to third countries under SCCs are presumably allowed unless a supervisory authority flags local law as sufficiently problematic both in probability and in magnitude.[142] This is a more lenient and flexible standard of legal sufficiency than that required for transfers under Article 45. The EC intended this lower threshold presumably to facilitate relatively low-risk data transfers to countries without an Article 45 adequacy approval.

2. The SCC 2.0

The SCC 2.0 approach the issue slightly differently but also embrace a risk-based approach to potential legal conflicts. First, the SCC 2.0 have jettisoned the language requiring either Party to warrant that the data 'will be processed in accordance with applicable data protection law' as a blanket matter. Instead, the Parties warrant only that they each will comply with data protections principles and their good faith belief that the law of the importing state does not prevent them from fulfilling their own obligations under the clauses.[143] That is a lower threshold.

In assessing this form of legal sufficiency the EC instructs the Parties to consider the laws of the destination country including any applicable limits or safeguards proposed in Annex I and II of the SCC.[144] They also may weigh the nature of the data flows, and factors such as, 'relevant practical experience with prior instances [of transfers], or the absence of requests for disclosure from public authorities . . . for the type of data transferred'.[145] This contextual inquiry is similar to the previous 'likely to have a substantial adverse impact' test from the earlier SCC decisions. It is certainly not a bright line rule that any possibility of access by third country law enforcement vitiates the protection of the Clauses.[146] The EC further instructs that Parties can consider the ability of technical and organizational measures to provide the necessary protection notwithstanding gaps in law.[147] The SCC 2.0 also spells out detailed obligations for importers and exporters in the event of legal conflicts or third country law enforcement requests for access. These obligations require transparency to exporters and data subjects about such requests, the duty to challenge overbroad requests, and prescribe use of data minimization and technological measures to safeguard rights in the event access cannot be avoided.[148] If the importer notifies the exporter of a deficiency in third country law that the exporter believes can be mitigated with technical and organizational measures, the exporter can notify the supervisory authority together

142 *Cf*. 1998 Report, *supra* note 111, at 12 ("Countries where the powers of state authorities to access information go beyond those permitted by *internationally accepted standards of human rights protection* will not be safe destinations for transfers based on contractual clauses.") (emphasis added).

143 Compare 2010 Clauses ¶ 4(a) with SCC 2.0 §II ¶ 2.

144 SCC 2.0 §II ¶2(b)(ii).

145 *Id.* at §II ¶2(b)(i).

146 The EDPB and the EDPS have noted the conflict with the EDPB Guidelines and have registered their objection to consideration of these "subjective" factors. EDPB-EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries 18–20 (Jan. 14, 2021) available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf.

147 *Id.* at §II ¶2(b)(iii).

148 SCC 2.0, at §II ¶3.

with a description of the applicable measures.[149] It would then be for the supervisory authority to suspend the transfer where it disagrees.[150] The SCC 2.0 framework is more demanding than the current SCCs but is still more forgiving than a full Article 45 legal adequacy ruling.

3. The CJEU and the EDPB Article 46 Adequacy Standard

The CJEU's *Schrems II* decision and the EDPB Guidelines are out of step with the EC's approach to appropriate safeguards and legal sufficiency under Article 46 in several important respects. First, as mentioned, the *Schrems II* standard for legal 'adequacy' under Article 46 is closer to the overall legal equivalency threshold required by Article 45(3). The test set forth in *Schrems II* and the EDPB Guidelines is purely a legal one: whether law enforcement powers 'go beyond what is necessary in a democratic society'.[151] The CJEU in *Schrems II* directs that a transfer should not proceed using SCCs if the law of that third country imposes 'obligations that are contrary to those clauses' and, therefore, are '*capable* of impinging on the contractual guarantee of an adequate level of protection'. (emphasis added)[152] The EDPB Guidelines similarly state that exporters should consider whether the law or practice of a third country 'may impinge' on protected rights.[153] The EDPB admonishes exporters to consider only 'objective' factors, such as the text of relevant legislation, and not 'subjective' determinations such as the likelihood that authorities will in fact access the data.[154] This is a bright-line approach, suitable for Article 45, rather than the more calibrated risk-based approach mandated for Article 46. In a pure law-based analysis under Article 45, any gap in protection or enforcement even if rare is unacceptable because in that event there is no effective redress in the importing country. Article 46 measures however, such as SCCs, already contain safeguards rooted in the domestic law of the exporter. In that case, a more pragmatic approach is warranted. For data transfers covered by SCCs, imposing liability on controllers for the mere possibility of access by a government authority is likely to lead to excessive caution without materially increasing the security of data subjects.

An 'objective' adequacy determination also may lead to some perverse decisions. In the first place, the EDPB Guidelines refer only to 'democratic societies'. Nearly half of the countries in the world are not organized as democracies or reflect features of both democracies and autocracies.[155] The Guidelines do not address the question of whether transfers to such states are permitted, or per se excluded. If excluded, it would prevent EU/EEA-based processors from processing personal data obtained in those third counties (eg in the context of a clinical trial or clinical research collaboration) and

149 *Id.* at §II ¶2(b)(f).

150 *But cf.* EDPB/EDPS Joint Opinion, *supra* note 146, at ¶¶ 92–95 (stating that there is no basis in the GDPR for a supervisory authority to undertake such a consultation, and asserting that the failure of a supervisory authority to object to a transfer after notification should not be taken as an authorization of that transfer).

151 Schrems II ¶ 36.

152 Schrems II ¶ 135.

153 EDPB Guidelines, *supra* note 2, at ¶ 30

154 *Id.* at ¶ 42.

155 Drew DeSilver, *Despite global concerns about democracy, more than half of countries are democratic*, Fact-Tank (May 14, 2019) available at https://www.pewresearch.org/fact-tank/2019/05/14/more-than-half-of-countries-are-democratic/.

transferring it back to the originating jurisdiction. If such transfers could proceed under Article 49's derogations, as the *Schrems II* decision indicates, it is not clear why they should always be forbidden under Article 46, when that section provides greater overall protection to data subjects than Article 49. Furthermore, while the text of legislation and decisions may seem an objective standard by which to judge legal sufficiency, it is also not always a good indicator of practice on the ground. Legislation may not be enforced as written. Restricting analysis to only 'objective' official evidence without consideration of the likelihood of access in practice could actually lead to a greater number of inappropriate transfers.[156]

It is not clear why the *Schrems II* ruling and the EDPB Guidelines ignore the significant non-legal safeguards within the SCCs that already mitigate any risks of misuse (eg Article 32, and the technical and organizational measures specified by the parties in Appendix 2 (Annex 2)). The CJEU states that, in the event of a legal conflict, the controller must provide 'additional safeguards to those offered by those clauses'.[157] This language indicates that the protections contained in the GDPR and the SCCs themselves are insufficient to compensate for the legal gaps and 'it may prove necessary to supplement the guarantees contained in those standard data protection clauses'.[158] The EDPB Guidelines similarly state that '[s]upplementary measures are by definition supplementary to the safeguards the Article 46 transfer tools already provide'.[159] However, Articles 24, 25, 28, and 32 together with clauses 4 &5 and Appendix 2 of the 2010 SCC Clauses (Section II and Annex 2 in the new versions), are already exhaustive. Clause 4(d) of the 2010 Clauses requires the exporter to undertake and ensure importer compliance with any technical and organizational 'security measures appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access, in particular where the processing involves the transmission over a network, and against all other unlawful forms of processing'.[160] It is uncertain what more a controller reasonably could adduce that would not already be captured by these requirements.

Finally, the *Schrems II* decision places the primary obligation to ensure legal adequacy on the exporter rather than the relevant supervisory authority. The decision states that 'it is 'above all for the controller . . . to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection'.[161] Only the largest and most sophisticated individual businesses can muster the resources to make such a determination with any degree of confidence. DPAs, by contrast, have the expertise and institutional capacity to evaluate whether foreign country rules are proportionate

156 The EDPB and the EDPS argue that consideration of subjective factors could prove very difficult and unverifiable. EDPB-EDPS Joint Opinion, *supra* note 146, at 19–20. Interestingly, they do note that in the absence of relevant legislation, actual practice by governmental authorities should be considered. *Id.* at [18]. However, they do not consider that seemingly 'objective' and verifiable factors such as the text of legislation may conflict with verifiable practice, nor do they prescribe a solution for when that is the case.

157 Schrems II, at ¶¶ 1, 134.

158 *Id.* at ¶ 132.

159 EDPB Guidelines, *supra* note 2, at ¶ 45.

160 2010 Clauses ¶ 4(d). This mandate is repeated in all versions of the SCC 2.0 in Section 2, Clause 1 "Security of Processing."

161 Schrems II ¶¶ 129–30, 134.

to democratic aims. It appears, post *Schrems II*, that controllers cannot simply refer such questions to supervisory authorities without making their own documented inquiry into legal adequacy first. This expense may restrict the ability of small and medium-sized EU entities to make use of the GDPR's transfer pathways.

In other Article 46 contexts, supervisory authorities continue to recognize the sufficiency of private contractual clauses, coupled with technological and organizational measures, even for transfers to US entities. European supervisory authorities approved, since July 2020, at least two transfers of EU subject personal data to the US under Article 47 Binding Corporate Rules (BCRs) and previous BCRs continue to be in effect.[162] BCRs are also contracts between private entities, specifically private companies under common control. Nothing in a BCR mitigates the risk that data will be accessed and surveilled under US security programs in a way different from SCCs. Nonetheless, supervisory authorities seem comfortable approving these contractual guarantees on the basis of technical guarantees and risk assessments about the kinds of data being exchanged. The EDPB Guidelines caution that supplementary measures may be necessary with all Article 46 safeguards, including BCRs.[163] However, to date (even following *Schrems II*), regulators do not seem to require additional language in the BCRs over and above preexisting guidance.[164]

New and more complex processing operations require risk-based and modular approaches to reducing the risks of transborder data flows. Analysis of law alone will not be sufficient to ensure important transborder information exchanges can continue regardless of national practices and political change. The approved and proposed SCCs under Article 46 already contain multiple safeguards ensuring compliance with GDPR standards even under inhospitable local law. As with Article 49, Article 46 provides an alternative pathway rooted in the exporter's domestic law to protect data subject rights that does not depend on the adequacy of protections in the importing state.

IV. SUPPLEMENTARY MEASURES

Notwithstanding the *Schrems II* decision, room remains to define 'supplementary measures' in a way that preserves their broad utility for many data flows, especially in well-regulated sectors such as health care. Unlike national laws, data processing technologies and information security systems are trending toward standardization. Adoption of third-party technical standards, codes of conduct and certification can provide the continuity of protection sought by the CJEU. In this section we set out recommendations for how privacy professionals and EU regulators can employ 'supplementary measures' to fill gaps in third country law consistent with the history and purpose of SCCs and the requirements of *Schrems II,* read narrowly. Tools such as Transfer Impact Assessments (described below) can build on the specific case analysis already mandated in Appendix 1 (Annex A) of the existing clauses. Additional terms requiring notice of and resistance to law enforcement requests for blanket data collection can reinforce the data subject

162 EDPB, Register of Approved Binding Corporate Rules, (Jotun & Tetrak July 30, 2020) https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en (*last visited* Nov. 7, 2020); Jetty Tielemans, *BCRs after 'Schrems II' decision: A first analysis*, IAPPS, https://iapp.org/news/a/binding-corporate-rules-after-the-schrems-ii-decision-a-first-analysis/ (Oct. 27, 2020).

163 EDPB Guidelines, *supra* note 2, at ¶¶ 58–59.

164 Tielemans, *supra* note 162.

rights contained in the main body of the SCCs. Appendix/Annex 2 of the Clauses can be enhanced through explicit reference to existing third-party standards, codes of conduct, privacy certifications, and other Security of Processing measures as laid out in Article 32 of the GDPR. These suggestions usefully can supplement the guidance provided by the EDPB. They may also be useful for the EC to consider as optional additions to the new draft clauses. The EC has an opportunity in the SCC 2.0 to mitigate the CJEU's narrow focus on legal adequacy and emphasize that effective data protection in a global context will depend on interlocking layers of modular and verifiable safeguards.

IV.A. Transfer Impact Assessments: A Case by Case Analysis of the Risks and Benefits of Transfer

If SCCs were ever considered 'off-the-shelf' solutions that could be employed without much effort, the *Schrems II* decision laid that misconception to rest. Appendix 1 (Annex A) already required parties to consider the nature of the personal data and the purposes of the transfer. Parties can supplement this analysis through use of what is becoming known as a 'Transfer Impact Assessment' (TIA).

Transfer Impact Assessments are not mentioned in the GDPR but are based on Data Protection Impact Assessments (DPIA) outlined in Article 35. DPIAs are required for processing activities that pose high risk to the rights and freedoms of natural persons.[165] They are often used when processing uses new technologies or sensitive data about a large number of people, but their use is not limited to such situations.[166] Article 35 requires that a controller 'shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data'. This Assessment should include (i) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller, (ii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes, (iii) an assessment of the risks to the rights and freedoms of data subjects, and (iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data.[167] Article 40 codes of conduct are mentioned in particular as useful risk mitigation measures.[168]

A TIA would consist of a similar analysis focused in particular on any risks posed by third country law and practice, and possible mitigations to those risks through SCCs, certification mechanisms and other targeted measures. The European Data Protection Supervisor, the data protection supervisor for EU institutions, office and agencies, has already issued guidance requiring its agencies to conduct TIAs for transfers to the USA or other third countries on a case by case basis.[169] A TIA would differ from a DPIA chiefly in its increased focus on (i) the nature of the data being transferred, (ii) the identity of the entity receiving the transfer, and (iii) the possible risks and protections contained in third country law.

165 GDPR Art. 35.
166 *Id.*
167 Art. 35(7)(d) GDPR.
168 Art. 35(8) GDPR.
169 European Data Protection Supervisor, *supra* note 96.

Several US agencies have issued a White Paper in the wake of *Schrems II* that illustrates the kind of information a country-specific TIA might contain.[170] First, the US White Paper notes that US law restricts the kinds of information that may be sought by intelligence agencies, and as a result, most commercial data exchanged across the Atlantic would be exempt from the government surveillance programs referred to in *Schrems II*. Where personal data concerns ordinary commercial information such as employee, customer or sales records, there is no basis to believe that US intelligence agencies would seek to collect that data.[171] Second, the White Paper notes limitations and protections present in US domestic law, both state and federal, that limit the ability of intelligence agencies to collect data and provide redress to foreign nationals in the event of overreach.[172] The agencies also listed alleged benefits to EU citizens as a result of national security data gathering, which they argued could provide a public interest basis justifying transfers to companies potentially subject to US government data-gathering requests.[173]

The US White Paper provided a general overview, but a specific TIA could go much further in considering both the risks and protections in relation to the kind of data being transferred and the identity of the recipient. With respect to data used in the provision of health care services, for example, US federal law already contains detailed protections and remedies against misuse via HIPAA's Privacy Rule.[174] In some cases these protections are supplemented by laws governing use of biometric or commercial data at the state level. The nature of the recipient and the purposes of processing also could be important. Medical entities in the USA engaged in clinical trials, for example, are subject to comprehensive patient data regulations via instruments such as the Food and Drug Administration Clinical Trial Regulations, and the Common Rule on Protection of Human Research Subjects. Furthermore, clinical trial regulations impose legal obligations on trial sponsors (and their contracted processors) to carry out certain data processing activities (eg analysis of safety and efficacy, safety reporting, archiving the clinical trial master file for 25 years) and to share data about clinical trial outcomes with medicine safety agencies.[175] Since data transfers required by law are specifically permitted by the GDPR, and such activities are circumscribed by the trial protocol, the risks of unduly extensive data processing are lower than in general personal data transfers. Other supplements include that trial sponsors being subject to inspections (eg Article 78 CTR) and audits,[176] and standards for Good Clinical Practice ('GCP'), which include standards relevant to data security and IT infrastruc-

170 U.S. Dept. of Commerce, *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for E.U.-U.S. Data Transfers after Schrems II* (Sept. 2020) available at https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.

171 *Id*. at [2].

172 *Id*. at [6–22].

173 *Id*. at [3–4].

174 Bradford, Aboy & Liddell, *supra* note 60, at 20–29.

175 Regulation (EU) No 536/2014 of the European Parliament and of the Council of April 16, 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, (2014) OJ L 158, 1–76 (Clinical Trials Regulation) https://ec.europa.eu/health/human-use/clinical-trials/regulation_en.

176 M. Corrales Compagnucci, T. Minssen, C. Seitz, & M. Aboy, *Lost on the High Seas without a Safe Harbor or a Shield? Navigating Cross-Border Transfers in the Pharmaceutical Sector After Schrems II Invalidation of the EU-US Privacy Shield* 4 Eur. Pharmaceutical L. Rev. 153, 157 (2020).

ture for multinational clinical trials.[177] Member State GCP inspectors are entitled to have access to clinical trial data, and to audit the protocol to ensure adherence to these standards.[178] All clinical trials under the CTR using human subjects also require research ethics approval, which will also consider how data are collected, used, and retained.

In the case of clinical trials, the risks of intelligence agencies seeking access to clinical trial data are small, and the benefits of sharing medical research data are many. A detailed TIA plus standard security measures such as minimization, pseudonymization, and encryption offer ample protection to the rights of EU subjects. In contrast, consider typical settings for consumer wearable devices. Companies in this industry are largely unregulated in the US. Yet they collect substantial quantities of health-related data that could attract the interest of law enforcement agencies. For instance, they collect information about an individual's daily biometrics and movements, sometimes via GPS. In such cases, the risks of a transfer is much greater.

The purposes and benefits of the transfer are also relevant considerations. Article 49 allows controllers to transfer personal data in the absence of an adequacy decision for certain defined purposes. These include where the data subject has knowingly consented to the transfer, where the transfer is necessary for performance of a contract or to protect the vital interests of the data subject, or for reasons of public interest such as exchange of information among tax, competition, or health authorities.[179] These transfers are allowed even where no appropriate safeguards and supplementary measures are present. It would make sense then that if Article 46 safeguards such as SCCs are also in place, transfers for similar purposes to those outlined in Article 49 should be permitted, even if some risk exists of conflict with local law.

IV.B. Contractual Supplementary Measures

In addition to TIAs, controllers can add (but not take away) legal obligations to the clauses themselves.[180] For example, with respect to French Health Data Hub, Microsoft Ireland promised not to process data outside the geographic area specified by the French authorities without prior approval.[181] It also promised to seek approval before providing data to its affiliates outside the EU, and to segregate more sensitive data before sharing data with affiliates for technical or billing purposes. Entities can also be required to disclose and challenge any law enforcement requests for access to the data. All of these contractual restrictions supplement the protections already contained within the existing default clauses. The EC's SCC 2.0 incorporate these requirements by default, as well as mandating contractual restrictions on the amount of time data can be stored and retained by the recipient organization. This is in keeping with the GDPR principle of 'data minimization'.

177 ICH Topic E 6 (R1): Guideline for Good Clinical Practice. CPMP/ICH/135/95, EMEA London, 1996/2002.

178 Compagnucci, Minssen, Seitz & Aboy, *supra* note 176, at 157.

179 GDPR Art 49 & Recital 112.

180 GDPR Recital 109.

181 Arrete, *supra* note 5, at 143.

Some companies have gone even further. On November 19, 2020, Microsoft announced additional new commitments that it would add to all public sector and enterprise cloud storage contracts. These included a promise to challenge any government request for public sector or enterprise customer data where a lawful basis exists for doing so. Second, Microsoft promised to provide financial compensation to users if it discloses their data in response to a government request in violation of the GDPR.[182]

Exporters can also add specific technical commitments of their own to Annex II of the SCC 2.0. The GDPR already requires data exporters to implement privacy by design and consider appropriate security measures. However, the SCC 2.0 for the most part refers only to importer obligations with respect to security of processing. By spelling out the exporter's obligations as well as part of the contract, exporters will give data subjects the additional avenues for enforcement of their rights via the third-party beneficiary clauses of the SCCs.

Exporters will need to consider the extent to which any additional supplemental measures in the form of contractual clauses could subject them to liability for the activities of the importing party as a joint controller.

IV.C. Technical and Organizational Safeguards

The final layer of protection for personal data sent across borders will be trusted and verified third-party standards for encryption and security of processing. Article 32 of the GDPR already requires use of technical and organizational protections to reduce any risk of transfer. The SCC 2.0 explicitly incorporates this mandate into the clauses, as does Appendix 2 of the existing controller to processor version. As the EPBD Guidelines note, technical measures such as encryption and pseudonimyzation, where the key to re-attributing the personal data remains under the exclusive control of the exporter, can ensure protection for data subjects even where legal protections are lacking.[183]

In addition to measures to cloak the data, Article 32 requires implementation of appropriate measures to protect the integrity of information management systems. A number of technical tools and standards exist to automate and augment such aspects of GDPR compliance. In particular, information security management systems (ISMS) and privacy information management systems (PIMS) standards such as those set by the International Organization for Standardization (ISO) are fast becoming accepted GDPR-friendly certification standards. ISO certification is a seal of approval from a third-party body that a company meets one of the international technical standards developed and published by the ISO. An ISO 27001 (ISMS) and ISO 27701 (PIMS) certification signals a commitment to a suite of state-of-the-art protocols and standards for data processing.[184] ISO standards are well-known and understood by businesses, and third-party conformity assessments are available worldwide.[185] Accordingly, the

182 Julie Brill, *New Steps to Defend Your Data, Microsoft Blog* (Nov. 19, 2020) available at https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/.

183 EDPB Guidelines, *supra* note 2, at Annex II Use Cases 1 & 2.

184 Dr. Eric Lachaud, ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification, 17 (2020).

185 *Id.* at [14].

IS0 27701 (the PIMS extension to the ISO 27001 ISMS) might become an approved GDPR 'certification mechanism' under Article 42 of the GDPR, which would create another 'appropriate safeguards' cross-border transfer mechanism under Article 46(f) GDPR.[186] Even without approval under Article 42, ISO certification can demonstrate good-faith compliance with GDPR Article 32 and Appendix 2 (Annex 2) of the SCCs.

Another technical measure that can facilitate some kinds of health research is a set of data management platforms that allow entities outside the EU to interrogate research findings without actually accessing any personal data. Data visitation through a thin client membrane allows visualization of the data but not retrieval, for example.[187] Another possibility is remote access via execution, wherein researchers use a synthetic version of a database to produce a query code/script for the analysis they wish to perform. The query is then run automatically or manually by the host institution and only results are shared with the outside research organization.[188] Infrastructure solutions such as DataSHIELD allow researchers to query data without accessing it and provide only anonymized results.[189] Such solutions are useful for longitudinal studies on the same large set of data or affiliated data hubs.

Use of technical measures, third party certifications, and data minimization techniques alongside TIAs and contractual restrictions can supplement the protections found in the default clauses and provide a pathway for transfers of important health data.

IV.D. Case Studies

The virtues of our approach, reflected in the SCC 2.0, can be seen by evaluating the ability to transfer data in three important health research scenarios discussed in Section 1 above:

1. A European organization asks a service provider located outside the EEA (eg a Clinical Research Organization; or the FDA) to process clinical trial data for the purposes of research or approvals.
2. Collaborative researchers located at institutes in Europe share and combine health data with researchers at American or Asian centers as part of long-term, longitudinal studies (eg an international rare disease consortium).
3. An EU entity sequences and analyzes genomic and other health data collected by partners in a less developed African country not recognized as adequate under the GDPR.

186 Compagnucci, Minssen, Seitz & Aboy, *supra* note 176, at 158.

187 Dara Hallinan et al., *International Transfers of Health Research Data Following Schrems II: A Problem in Need of a Solution*, (Draft) at 17; *but see* EDPB Guidelines *supra* note 2, at ¶ 13 (noting that remote access from outside the EEA could also be considered a transfer).

188 Hallinan et al., *supra* note 187, at 18–19.

189 *Id.*

As each of these scenarios involves repetitive transfers, Article 49's derogations would not be available.[190] Without an Article 45 adequacy determination, the sole possibility would be an Article 46 pathway. Below we summarize how the various regulatory authorities in the EU would approach these issues post-*Schrems II*.

CNIL (French supervisory authority)

The French supervisory authority, CNIL, would allow no transfers of personal data to entities outside the EEA or subject to non-EEA law. According to CNIL, EU personal data must be processed by entities subject to EU law alone. Therefore, none of the three types of health transfers are permissible. Once an entity subject to foreign law accesses the personal data, the full protections of the GDPR have been compromised. This interpretation of *Schrems II* would lead to siloed research efforts and would undercut collaborative responses to public health challenges such as COVID-19. EU/EEA organizations (eg universities, pharma, medical device companies, technology providers) would be prevented from processing personal data from third countries, as once the data are processed in the EU/EEA and subject to GDPR, it would not be possible to transfer it back to the third country where the personal data were originally collected (eg an African country). Accordingly, these international research collaborations would need to exclude EU/EEA organizations in favor of controllers and processors established in other jurisdictions such as the USA or other Asia Pacific Economic Cooperation member countries.

EDPB Guidelines

The EDPB Guidelines allow personal data to be transferred to a jurisdiction outside the EEA under Article 46 only if that government's authorities do not engage in blanket surveillance for national security purposes or if technical safeguards effectively prevent access to personal data by those authorities. Since a contracting party cannot promise to disregard the mandates of its own government, in practice this means data must be encrypted and pseudonymized with the reidentification key remaining in Europe. This would allow the use of information technology service providers, such as Microsoft or Amazon Web Services, to host encrypted data on behalf of EEA controllers. However, collaborative projects such as the second research scenario would not be possible if the reidentification key is shared with a partner, and the law of the partner jurisdiction falls short of the CJEU's legal equivalency threshold. Therefore, EEA researchers may find it difficult to partner with and share results with entities in the USA or Asia for the purposes of health research. In the third scenario, once the health data from the developing country arrived in Europe for processing, it would be subject to the GDPR. Therefore, the EU entity could not return the results in unencrypted form with the local agencies that collected the data or even with the African data subjects themselves.[191]

190 *See* Bradford, Aboy & Liddell, *supra* note 62, at 9–10.

191 *See* EDPB Guidelines 7/2020, *supra* note 22, at 13 (noting that EU entities engaging in processing tasks for non-EU entities are subject to the transfer restriction provisions of Chapter 5 of the GDPR).

SCC 2.0

All three data flows can proceed, subject to safeguards. The clinical trial data in the first research scenario could be shared with service providers in encrypted and pseudonymized form, with the reidentification key remaining in Europe. The research partnership in the second scenario could continue, subject to GDPR organizational commitments and adherence to data minimization and privacy by design principles. The EU processing entity in the third scenario could sequence the African genomic data and return the results to the originating institution subject to the applicable SCC 2.0 safeguards. If the genomic data were combined with EU subject personal data, then both institutions would need to institute Article 46 safeguards to share the pooled data including the necessary supplementary measures in the event of African government access requests.[192]

V. CONCLUSION

SCCs and other Article 46 'appropriate safeguards' provide a multi-layered approach to data protection that relies on law, technology, and organizational commitments to create an appropriate environment for international data transfer. Their purpose is to bridge gaps in situations where the legal framework of the importing country alone would be insufficient to protect data subject rights. As such, they embody the future of cross-border privacy protection as a set of modular, contextual, and risk-based mechanisms that can be tailored to suit particular data flows.

GDPR restrictions on cross-border transfers of personal data ensure a consistent and high-level of protection for personal autonomy and privacy. However, restrictions on transfer are not the primary mechanism through which this level of protection is guaranteed. The GDPR has a considerable extra-territorial reach that already lowers the risk misuse of personal data outside the borders of the EEA. The GDPR's transfer restrictions should be understood as a limited additional layer of protection that lowers, but does not completely eliminate, risks posed by inconsistent law or prying governments.

The GDPR allows transfers outside the EEA under three alternate conditions. Article 45 GDPR allows transfers to jurisdictions found by the EC to offer essentially equivalent legal protections for data subjects to those found in the GDPR. The exporter and importer are not required to put special measures in place because the data protection standards in the importing country have already been judged adequate. Article 49 allows transfers in compelling circumstances, even where the rights of data subjects might be put at risk, but not on an on-going basis. Special measures are not required because these transfers are exceptional only. Finally there is Article 46, which allows transfers on an on-going basis, when the importing country does not have an adequacy decision. Article 46 does not require the importing country to have full equivalency in its legal framework but it instead imposes safeguards through technical and organizational means and via effective legal remedies under the law of the exporting country.

192 SCC 2.0 § II ¶ 3.

The *Schrems II* case was a missed opportunity to clarify how these different transfer mechanisms interact. Instead, the court repudiated or made unstable the two principal mechanisms for data transfers to third countries. First, the ruling tightened the meaning of 'adequacy' under Article 45 to the point where several existing adequacy rulings are now in doubt. Second, the CJEU also seemed to define accountability under Article 46 so broadly as to include responsibility for ensuring stringent adequacy of the importing country's law. Such a broad ruling threatens to have Article 45's adequacy test swallow the rest of the transfer mechanisms. Indeed, some regulators have interpreted the decision as essentially banning transfers to inadequate jurisdictions under any circumstances.

We argue that Article 46 safeguards such as SCCs offer a distinct pathway for transfers to jurisdictions without Art 45 'legal adequacy', based on the application of the GDPR in the domestic law of the exporting country, the extra territorial reach of the GDPR and additional technical and organizational means specified in the SCCs. The appropriate safeguards provided by the standard clauses are three-fold. First, Annex/Appendix 1 requires the Parties to consider and demonstrate compliance with the GDPR's governing principles. Second, the clauses themselves ensure enforceable data subject rights and effective remedies under the exporter's domestic law. Third the Clauses require the parties to analyze the contemplated data flow and identify technological and organizational measures that are appropriate to address specific risks. The result is a multi-faceted and layered approach to protection that does not depend on rights in the importing state. These interconnecting layers of protection are retained in the EC's proposed SCC 2.0.

The EC has made clear that it did not intend to make strict legal equivalency in the importing country a pre-condition for transfer under Article 46. Instead, the EC implementing decisions for the existing SCCs and the SCC 2.0 lay out a risk-based approach when the SCC clauses apply. In particular, the SCC implementing decisions point to an advisory role for supervisory authorities in weighing whether conflicts with third country law justify the suspension or prohibition of data flows or whether SCCs and supplementary measures sufficiently mitigate risks. This is a more permissive stance than that taken in the EDPB Guidelines after *Schrems II*. The EC's approach makes sense considering (i) the broad extra-territorial reach of the GDPR, (ii) the multiple safeguards already operating within the SCCs to limit unwarranted access to protected data and (iii) the multiple GDPR protections that apply in the domestic law of the exporting country.

Supplementary measures can enhance these safeguards further. Going forward, reliance on industry-specific codes of conduct and third-party certifications can lower the burdens of GDPR compliance even further for smaller and medium sized entities. Thorough Transfer Impact Assessments can assure tailored and appropriate use of technological and organizational controls. Additional contractual clauses requiring resistance to government access requests and reaffirming GDPR security of processing obligations can provide further reassurance to data subjects. In conjunction with these additional guarantees, SCCs should continue to provide relatively straightforward safe harbor transfer mechanisms for many kinds of data, including regulated health data.

ACKNOWLEDGEMENTS

The authors thank anonymous reviewers for their helpful comments. The authors acknowledge the support by the Novo Nordisk Foundation for the scientifically independent Collaborative Research Program for Biomedical Innovation Law (grant NNF17SA0027784).