CENTRE FOR THE LAW OF EU EXTERNAL RELATIONS

CLEER

The Application of EU Law Beyond Its Borders

Federico Casolari and Mauro Gatti (eds.)

CLEER PAPERS **2022/3**

CENTRE FOR THE LAW OF EU EXTERNAL RELATIONS

THE APPLICATION OF EU LAW BEYOND ITS BORDERS

FEDERICO CASOLARI AND MAURO GATTI (EDS.)

CLEER PAPERS **2022/3**

Editorial policy

The governing board of CLEER, in its capacity as board of editors, welcomes the submission of legal papers and commentaries (max. 40,000 resp. 4.000 words, incl. footnotes, accompanied by keywords and short abstracts) at E.Kassoti@asser.nl. CLEER applies a double blind peer review system. When accepted, papers are published on the website of CLEER.

ISSN 1878-9587 (print)
ISSN 1878-9595 (online)

Printed in The Netherlands
T.M.C. Asser Institute
P.O. Box 30461
2500 GL The Hague
The Netherlands
www.cleer.eu

CONTENTS

INTERNATIONAL TRANSFERS OF DATA CONCERNING HEALTH AFTER SCHREMS II: A NEED FOR SECTOR-SPECIFIC LEGAL AVENUES AND SUPPLEMENTARY MEASURES

Richard Rak*

1. INTRODUCTION

International (transborder, cross-jurisdictional) transfers of data concerning health may be necessary for a wide range of purposes.[1] The fight against the coronavirus pandemic has highlighted the importance of international data collaborations in developing medicinal products and medical devices. As health data ecosystems expand, an increasing number and variety of stakeholders have become involved in the processing of data concerning health across different jurisdictions.[2] This expansion is taking place as health data flows are becoming ubiquitous in nature.[3] This transformation is driven by the implementation of the Internet of Things (IoT) as an enabling technology in healthcare, which aims to exploit 'network effects' in order to support decisions affecting the

* University of Vienna, University of Bologna and University of Turin, PhD Candidate in Law, Science and Technology. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Marie Skłodowska Curie grant agreement no. 814177.

[1] The main purposes for processing data concerning health in a different jurisdiction are:
a) provision of patient care;
b) assessment of health insurance coverage and payment for care provision;
c) health service management and quality assurance;
d) public health surveillance and disease control;
e) public safety management;
f) population health management;
g) scientific research (clinical trial); or
h) market study (See International Organization for Standardization, *ISO/TS 14265:2011(en) Health Informatics – Classification of purposes for processing personal health information*, Annex A).

[2] Various types of entities may be involved in receiving data concerning health from another jurisdiction, in particular:
a) healthcare establishments;
b) public authorities;
c) health insurance funds;
d) contractors remotely maintaining health information systems;
e) researchers (research databanks);
f) organisations holding educational databases;
g) companies (e.g. employers, ICT solution providers) holding electronic health datasets; or
h) organisations engaged in health-related e-commerce (e.g. e-pharmacy) activities (See International Organization for Standardization, *ISO 22857:2013(en) Health informatics – Guidelines on data protection to facilitate trans-border flows of personal health data*, Introduction).

[3] C. Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future*, OECD Digital Economy Papers, No. 187 (Paris: OECD Publishing 2011), at 10-11.

health of citizens/patients by delivering the right information to the right person (or machine) at the right time and in the right place.[4] The rapid scaling of IoT-enabled telehealth solutions during the pandemic has accelerated these developments.[5] These changes are intensifying the volume and complexities of international transfers of data concerning health, increasing the urgency of improving the underlying legal, technical and organisational arrangements.

In general, growth in cross-jurisdictional data transmissions has led to the adoption of privacy and data protection laws establishing conditions for international transfers of personal data. Globally, there seems to be a growing trend towards stricter requirements, reflected by the inclusion of many General Data Protection Regulation[6] (GDPR)-like principles in newly adopted or revised legislations outside the EU/EEA.[7] The protection of personal data and extraterritorial enforcement of privacy and data protection laws have become matters of strategic importance for countries and international alliances. In this regard, the policy goal is to counter risks that may arise from transfers of personal data to a different jurisdiction, notably:[8]

- to prevent the circumvention of domestic or supranational privacy and data protection laws;
- to guard against data processing risks in other jurisdictions;
- to assert privacy and data protection rights in other jurisdictions; and
- to enhance the confidence of individuals.

In order to ensure that two jurisdictions applying two different privacy and data protection laws can act harmoniously, it is fundamental for there to be, in principle, a degree of commonality which is either recognised or achieved.[9] Although the core principles of privacy and data protection tend to remain fairly consistent from jurisdiction to jurisdiction, when significant differences do appear, privacy and data protection rules may transform into barriers to transborder data flows.[10]

---

[4] See CISCO Systems, *White Paper: The Internet of Everything (IoE) and the Delivery of Healthcare*, CISCO Systems (2015), available at <https://www.himss.eu/content/cisco-white-paper-internet-everything-ioe-and-delivery-healthcare>.

[5] See O. Bestsennyy *et al*., Telehealth: A quarter-trillion-dollar post-COVID-19 reality?, McKinsey & Company (29 May 2020), available at <https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality>.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ* [2016] L 119/1, 4.5.2016 (hereafter: General Data Protection Regulation).

[7] G. Greenleaf, 'Global Data Privacy Laws 2019: 132 National Laws & Many Bills', 157 *Privacy Laws & Business International Report* 2019, 14-18 at 18.

[8] C. Kuner, *Transborder Data Flow Regulation and Data Privacy Law* (Oxford: Oxford University Press 2013), 107-119.

[9] World Economic Forum, *A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy* (Geneva: World Economic Forum, 9 June 2020), at 23, available at <http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf>.

[10] Ibid., at 21.

These rules may act as 'hard barriers' if asymmetry exists between legal frameworks (i.e. differences in the legal conditions for transfers of data concerning health, such as the level of protection offered to data concerning health in the respective jurisdictions). Alternatively, they may become 'soft barriers' if they establish extra requirements for compliance (e.g. a complex legal procedure for transfers of data concerning health is likely to cause additional administrative and financial burdens for the parties involved).

In this case, legal and practical compliance challenges have posed barriers, which are discouraging transfers of data concerning health from the EU/EEA to third countries. As the Commission has not recognised many of the world's biggest economies as offering an adequate level of data protection, but it is fair to assume that intensive transborder data flows are taking place, there are doubts about the correct implementation of the respective privacy and data protection rules and the level of compliance in practice.[11] Inconsistencies in the authoritative interpretations of the GDPR and the absence of sector-specific guidance on transfers of data concerning health outside the EU/EEA have compounded the legal uncertainty. Such a lack of predictability creates problems not only for data exporters in EU/EEA health data ecosystems, but also for data importers in non-EU/EEA jurisdictions, as well as international organisations, whose work might be hindered.[12] In its landmark ruling in *Schrems II*, the Court of Justice of the European Union (CJEU) made several significant rulings on the proper interpretation and application of the legal framework regulating the requirements for transfers of personal data from the EU/EEA to third countries or international organisations.[13] The objective of this article is to outline the legal and practical consequences of *Schrems II* and subsequent case law, authoritative legal interpretations and normative acts relating to the establishment of requirements for transfers of data concerning health outside the EU/EEA. Based upon these findings, the article argues that sector-specific legal avenues should be adopted and appropriate supplementary measures should be implemented in order to overcome the barriers that are currently hindering international transfers of data concerning health from the EU/EEA.

[11] See C. Kuner, *supra* note 8, at 146; R. H. Weber, 'Transborder data transfers: concepts, regulatory approaches and new legislative initiatives', 3 *International Data Privacy Law* 2013, 117-130, at 124.

[12] See J. Stoddart *et al.*, 'The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research', 44 *The Journal of Law, Medicine & Ethics* 2016, 143-155, at 146.

[13] Court of Justice of the European Union, Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2020], Judgment of the Court (Grand Chamber) of 16 July 2020, ECLI:EU:C:2020:559 (hereafter: *Schrems II Case C-311/18*).

2. LEGAL APPROACHES AND AVENUES FOR TRANSFERRING DATA CONCERNING HEALTH OUTSIDE THE EU/EEA

2.1. **Legal approaches for regulating international transfers of personal data**

There are two major legislative models that regulate international transfers of personal data (concerning health). It is important to examine them in order to ascertain the underlying policy considerations:[14]

a) The geographical (or jurisdictional) approach[15] aims to protect against risks posed by shortcomings of the legal system in the country or territory to which personal data (concerning health) are to be transferred. This approach is based on a comparative legal assessment of the level of data protection offered by the jurisdictions of the data exporter and the data importer. In order for this evaluation of adequacy or comparability to be amended, a formal review of the comparative legal assessment must be carried out. The drawback of this approach is that since private actions do not have a direct influence on the status of the law, this model does not take account of any special efforts made by the parties concerned.
b) The organisational (or accountability) approach[16] requires the data exporter to perform its own *ad hoc* assessment and to determine the safeguards needed in order for the transfer to be deemed permissible. This requirement makes organisations accountable for guaranteeing the continuous protection of personal data (concerning health) when those data are transferred to other organisations, irrespective of their geographical location. The appropriate level of safeguards is designed and implemented by the data exporter and data importer either on a contractual basis or through self-regulation or co-regulation. This approach is based on the idea of corporate due diligence.[17] Although there is a 'business case' to promote corporate due diligence and accountability, this model places significant burdens on organisations and enforcement authorities.

---

[14] See C. Kuner, *supra* note 5, at 20; R. H. Weber, *supra* note 11, at 122; M. Phillips, 'International Data-Sharing Norms: from the OECD to the General Data Protection Regulation (GDPR)', 137 *Human Genetics* 2018, 575-582, at 576.

[15] Regulatory examples include: General Data Protection Regulation (*supra* note 6); Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data – Consolidated text, ETS No. 223, 128th Session of the Committee of Ministers (Elsinore, 17-18 May 2018).

[16] Regulatory examples include: Organisation for Economic Co-operation and Development, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79]; Asia-Pacific Economic Cooperation (APEC) Privacy Framework (2015) and Cross-Border Privacy Rules (CBPR) System.

[17] C. Bennett and S. Oduro-Marfo, 'GLOBAL Privacy Protection: Adequate Laws, Accountable Organizations and/or Data Localization?', *UbiComp '18: Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers* (Singapore, October 2018) (New York: Association for Computing Machinery), 880-890, at 887.

Neither of the two approaches exists in its 'pure' form. Most normative instruments combine these two models in different ways, partly because the geographical approach is losing relevance due to the globalisation of communication channels and data flows.[18] Either of these default approaches can work insofar as they are accompanied by appropriate measures to limit their inherent disadvantages; otherwise, the geographical approach tends to be too reactive, while the organisational approach can become excessively bureaucratic for organisations.[19] Although there is a tendency to proclaim (prescriptive) jurisdiction extraterritorially (referred to as 'regulatory overreaching')[20], the reality is that there is no prospect of exercising (adjudicating or enforcing) some jurisdictional claims. This phenomenon is described as 'bark jurisdiction', as opposed to 'bite jurisdiction'.[21] However, it should be noted that, internationally, the importance of enforceability often lies not in inducing a fear of sanctions in the event of non-compliance but, rather, in affirming a foreign law's legitimacy or political influence.[22]

2.2. Legal avenues offered by the GDPR for transferring personal data (concerning health) from the EU/EEA to third countries or international organisations

Chapter V of the GDPR establishes three main legal avenues ('data transfer mechanisms' or 'transfer tools') for transferring personal data from the EU/EEA to third countries or international organisations. These legal avenues also apply to transfers of data concerning health outside the EU/EEA on the condition that the processing of data concerning health is based on a legal ground established in Chapter II of the GDPR. The legal avenues constitute a three-layered hierarchy of rules:

1. 'transfers on the basis of an adequacy decision' by the Commission (Article 45);
2. in the absence of an adequacy decision, 'transfers subject to appropriate safeguards' by the data exporter (controller or processor) on the condition that data subjects' rights can be enforced and effective legal remedies are available for data subjects (Article 46); and
3. in the absence of the foregoing legal avenues, 'derogations for specific situations' may be permitted for which the legislator has decided that the balance of interests allows a data transfer under certain conditions (Article 49).

---

[18] R. H. Weber, *supra* note 11, at 123.

[19] C. Kuner, *supra* note 5, at 27.

[20] L. Bygrave, 'European Data Protection: Determining Applicable Law Pursuant to European Data Protection Legislation', 16 *Computer Law & Security Review* 2000, 252-257, at 255; see, also, General Data Protection Regulation, *supra* note 6, Article 3.

[21] D. J. B. Svantesson, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses', 50 *Health Policy and Technology* 2014, 53-102, at 58-59.

[22] U. Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (Cambridge: Cambridge University Press 2007), at 205.

In effect, these mechanisms are aimed at ensuring that either the country/jurisdiction (adequacy decision) or the organisation (appropriate safeguards) guarantees an appropriate level of data protection to the data subject.[23] If neither of these requirements is satisfied and there is no situation for permissible derogation, the only way to transfer data concerning health outside the EU/EEA is to render the data anonymous, so that the GDPR no longer applies.

3. *SCHREMS II* AND ITS IMPLICATIONS ON TRANSFERS OF DATA CONCERNING HEALTH OUTSIDE THE EU/EEA

The *Schrems II* judgment[24] was an important milestone in the case law of the CJEU concerning transfers of personal data outside the EU/EEA. The crux of the case was to decide whether the EU-US Privacy Shield adequacy decision and the standard data protection clauses adopted by the Commission guarantee legal protection in light of the fact that US law allows public authorities to access personal data without establishing any limitations on the power it confers to implement surveillance programmes. The CJEU decided to invalidate the EU-US Privacy Shield having found that US law did not offer an 'essentially equivalent' level of protection in providing 'appropriate safeguards', 'enforceable rights' and 'effective legal remedies', as required by the GDPR, read in the light of the Charter of Fundamental Rights of the European Union.[25] Nonetheless, the CJEU held that the standard contractual clauses in force for transfers of personal data to processors established in third countries should remain valid, but their application may require the adoption of supplementary measures by the controller in order to ensure compliance with the level of protection required under EU law.[26]

As regards the consequences of *Schrems II*, the immediate effect is that there is no longer an adequacy decision in force for justifying transfers of data concerning health between the EU and the US. The inability of relying on a predictable mechanism for data transfers has the effect of reducing health data collaborations between the EU and the US (and the rest of the world), which may ultimately lead to the cessation of critical data flows or harmful delays in the same.[27] This obstacle has serious legal and economic consequences for a wide range of entities, which would otherwise rely on an effective transfer mechanism between the EU and the US.[28] The stakeholders directly affected

---

[23] L. Bradford *et al*., 'International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an 'adequate' level of protection', lsaa055 *Journal of Law and the Biosciences* 2020, at 6.

[24] *Schrems II* (*supra* note 13).

[25] Ibid., para. 105.

[26] Ibid., para. 133.

[27] J. Bovenberg *et al*., 'How to fix the GDPR's frustration of global biomedical research', 370 *Science* 2020, 40-42, at 41-42.

[28] T. Minssen *et al*., 'The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR. What are the legal challenges and how might these affect cloud-based technologies, big data, and AI in the medical sector?', 4 *European Pharmaceutical Law Review* 2020, 34-50, at 46.

include *inter alia* researchers, pharmaceutical companies and organisations involved in providing new health information technologies. The European research-based pharmaceutical industry has expressed its concern that despite the multiple additional safeguards in place for the protection of data concerning health (such as research ethics procedures and Good Clinical Practice frameworks), the requirement to carry out case-by-case adequacy assessments is too burdensome for the industry.[29] This heavy burden means that data exporters have to spend significant amounts of supplementary resources on conducting legal assessments necessary to ensure the proper justification of data transfers under Article 46 of the GDPR.[30] However, many organisations seeking cross-Atlantic health data collaboration might not possess the resources required to perform these assessments; or, if they do, they then need to perform cost-benefit analyses to ascertain whether or not to allocate these resources for such purposes.[31]

4. THE IMPACT OF *SCHREMS II* ON SUBSEQUENT CASE LAW AND NORMATIVE INTERPRETATIONS RELATING TO THE JUSTIFICATION OF TRANSFERS OF DATA CONCERNING HEALTH OUTSIDE THE EU/EEA

4.1. **Recommendations 01/2020 issued by the European Data Protection Board**

As a follow-up to *Schrems II*, the European Data Protection Board (EDPB) issued *Recommendations 01/2020* in order to provide a roadmap for controllers and processors (acting as data exporters) to follow a series of steps in adopting appropriate supplementary measures, where necessary.[32] Essentially, this roadmap establishes the requirement for data exporters to conduct a 'transfer impact assessment'.[33] As regards 'supplementary measures', they are, by definition, supplementary to the safeguards already envisaged by the Article 46 GDPR transfer tool.[34] The EDPB drew on the principle of accountability to call on controllers and processors to demonstrate their data protection efforts to data subjects, the public, and data protection supervisory authorities.[35] The EDPB noted

[29] B. Barnes, 'International Transfer of Health Data Cross-Sectoral Roundtable – Summary Report', *Federation of European Academies of Medicine (FEAM) European Biomedical Policy Forum* (16 October 2020), at 4-5, available at <https://www.feam.eu/wp-content/uploads/ITHD-Summary-report-5-Nov-2020-FINAL.pdf>.

[30] D. Hallinan *et al*., 'International Transfers of Health Research Data following Schrems II: A Problem in need of a Solution', *European Journal of Human Genetics* 2021, at 4.

[31] Ibid.

[32] European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (10 November 2020) (hereafter: EDPB Recommendations 01/2020), at 6 (Recital 8) and 8 (para. 6).

[33] European Data Protection Supervisor, Preliminary Opinion 8/2020 on the European Health Data Space (17 November 2020), at 12-13 (para. 38).

[34] See General Data Protection Regulation (*supra* note 6), Recital 109; *Schrems II* (*supra* note 13), para. 133.

[35] EDPB Recommendations 01/2020 (*supra* note 32), at 7 (para. 3).

that the principle of accountability is necessary in order to ensure effective application of the level of protection conferred by the GDPR, as accountability also applies to data transfers to third countries (and onward transfers), with data transfers being a type of data processing in themselves.[36] Drawing on the principle of accountability could facilitate improved responses to new information technology developments and could make EU/EEA data protection rules more interoperable globally.[37] In this regard, the EU/EEA should consider that interoperability – not harmonisation or adequacy – is the key objective of the APEC Cross-Border Privacy Rules[38] (CBPR), which are generally more appealing from a corporate perspective, as they are less complex and prescriptive to respect and more facilitative of transborder data flows.[39]

4.2. The ruling of the French Council of State concerning the French Health Data Hub and Microsoft Ireland

Schrems II prompted several legal cases at national level of significance to transfers of data concerning health outside the EU/EEA. Following the CJEU's judgment, the French Council of State (*Conseil d'État*) was asked to rule on the legality of the French Health Data Hub (Hub).[40] According to the applicants, there was a risk of the right to privacy and the right to protection of personal data being violated in the processing and centralisation of data concerning health in the Hub with regard to the COVID-19 epidemic. Previously, the Hub had concluded a contract with Microsoft Ireland Operations Ltd, a company incorporated under Irish law. Under this contract, Microsoft Ireland licensed software necessary to process data concerning health collected by the Hub, and it stored and made available these data from its data centres located in the Netherlands. The applicants argued that significant legal risks were posed by the fact that Microsoft Ireland was a subsidiary of Microsoft Corporation, a company incorporated under US law and therefore subject to US surveillance laws.

In its judgment, the *Conseil d'État* noted that in *Schrems II* the CJEU only ruled on the conditions under which transfers of personal data to the US may take place, but did not rule on the conditions under which such data may be processed within EU territory by companies incorporated under US law or their subsidiaries.[41] In this regard, the *Conseil d'État* went even further than the CJEU by ruling in a case where data concerning health were processed by the

---

[36] Ibid., at 7 (para. 4) and 9 (para. 10).

[37] N. Cory *et al*., 'Principles and Policies for "Data Free Flow With Trust"', *Information Technology & Innovation Foundation* (27 May 2019), at 9, available at <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

[38] See *supra* note 16.

[39] C. Sullivan, 'EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era', 35 *Computer Law & Security Review* 2019, 380-397, at 385.

[40] Conseil d'État [Council of State of the French Republic], Case No. 444937, *Association Le Conseil National du Logiciel Libre et autres* [2020], Ordonnance of 13 October 2020, ECLI:FR:CEORD:2020:444937.20201013.

[41] Ibid., para. 18.

subsidiary of a company subject to the surveillance laws of a third country. The *Conseil d'État* pointed out that the applicants did not allege a direct violation of data protection rules, but only the risk of such a breach.[42] It also found that there is an important public interest in allowing the continued use of data concerning health for the purpose of health emergency management and improvement of knowledge about COVID-19 and, to this end, in permitting the use of the state-of-the-art technical means made available to the Hub by Microsoft Ireland.[43] In this case, contracting with Microsoft Ireland is a measure proportionate to the health risks incurred and is appropriate to the circumstances taking account of both the urgency and the absence of a satisfactory alternative technical solution facilitating the performance of tasks within the necessary time limits.[44] The *Conseil d'État* highlighted that the contract with Microsoft Ireland stipulates that data may not be processed outside the specified geographical zone (the Netherlands). [45] With regard to those considerations, the *Conseil d'État* found that it was satisfactory for the Hub to undertake to collaborate with Microsoft Ireland, under the supervision of the French Data Protection Authority, on implementing technical measures and appropriate organisational structures in order to guarantee the protection of the rights of the individuals concerned.[46]

4.3. The ruling of the French Council of State concerning Doctolib and AWS

In another case (based on similar arguments), the applicants asked the *Conseil d'État* to suspend the contract between the Minister of Health and Solidarity and Doctolib, an online platform assigned to manage the scheduling of vaccination appointments in France.[47] Doctolib used the hosting services of AWS Sarl, a company incorporated under Luxembourg law and a subsidiary of Amazon Web Services Inc., a company subject to US surveillance law. The applicants claimed that the partnership with Doctolib was not necessary, proportionate or appropriate given that there were other alternative digital solutions. In view of the data concerned and the implemented safeguards, the *Conseil d'État* found that the level of protection offered to data in the context of the COVID-19 vaccination campaign could not be regarded as manifestly insufficient in light of the risk of infringement of the GDPR.[48] The *Conseil d'État* held that the data at issue included personal identification data and data relating to appointments, but did not include any health data on the possible medical reasons for vaccination eligibility.[49] The *Conseil d'État* considered the complementary addendum on

[42] Ibid., para. 19.
[43] Ibid., para. 20.
[44] Ibid.
[45] Ibid., para. 12.
[46] Ibid., para. 21.
[47] Conseil d'État [Council of State of the French Republic], Case No. 450163, *L'association InterHop et les autres* [2021], Ordonnance of 12 March 2021, ECLI:FR:CEORD:2021:450163.20210312.
[48] Ibid., para. 9.
[49] Ibid.

data processing between Doctolib and AWS as providing a sufficient level of protection. In this addendum, the parties established a specific procedure for challenging any request made by a public authority to access data processed on behalf of Doctolib that did not comply with EU law.[50] In addition to this, Doctolib set up a data security system hosted by AWS in its data centres in France and Germany, through an encryption procedure based on a trusted third party located in France, in order to prevent the data from being seen by third parties.[51]

4.4. The decision of the Portuguese Data Protection Authority concerning the Portuguese National Statistical Institute

In a substantially different case, the Portuguese Data Protection Authority (CNPD) ordered the Portuguese National Institute for Statistics (INE) to suspend any transfers of personal data (including data concerning health) collected by INE in the 2021 Census to third countries that did not guarantee an adequate level of data protection.[52] INE had used the cyber security and Content Delivery Network services of Cloudflare, a company subject to US surveillance law. INE had accepted Cloudflare's terms and conditions relying on standard data protection clauses for transferring personal data to third countries. However, this contract allowed the transit of personal data through servers used by Cloudflare located in the US and other third countries, which did not offer an adequate level of protection. The contract also authorised Cloudflare to use sub-processors from outside its group, including third country companies. The contract noted that Cloudflare may be subject to data disclosure requests by the US government, which may be inconsistent with the GDPR, and those requests may prohibit the controller from being notified. In its assessment, the CNPD found that despite the use of standard data protection clauses, INE did not implement adequate and sufficient supplementary measures, which would have ensured an equivalent level of protection for transfers of personal data to third countries.[53] Moreover, INE did not carry out a Data Protection Impact Assessment for this specific processing operation and did not consult the supervisory authority prior to processing.[54]

[50] Ibid.
[51] Ibid.
[52] Comissão Nacional de Proteção de Dados [National Data Protection Commission of the Portuguese Republic], Deliberação/2021/533, 27 April 2021, AVG/2021/401, para. 42.
[53] Ibid., para. 30-40.
[54] Ibid., para. 20.

5. THE NEED FOR SECTOR-SPECIFIC LEGAL AVENUES AND SUPPLEMENTARY MEASURES TO FACILITATE LAWFUL TRANSFERS OF DATA CONCERNING HEALTH OUTSIDE THE EU/EEA

5.1. **Transfers on the basis of an adequacy decision by the Commission in the healthcare sector**

An adequacy decision offers the most comprehensive, straightforward and cost-effective solution for transferring personal data (concerning health) outside the EU/EEA.[55] It "assimilates" data transfers to intra-EU/EEA data transmissions in order to provide legal certainty and uniformity throughout the EU/EEA regarding the adequate level of protection offered by the other jurisdiction. Despite its advantages, this legal avenue has several weaknesses. The adequacy assessment procedure was designed to satisfy a far simpler and largely bilateral international environment for personal data transfers.[56] It is less suited to coping with a ubiquitous and multi-directional digital sphere labelled as the 'Internet of Everything'. In connection with this, it is important to note that the image of 'movement' given by the notion of 'data transfers' is not, in reality, actually the movement or transfer of data but actually data processing operations typically consisting of data replication or remote processing operations.[57]

The GDPR permits adequacy decisions in relation to one or more specified sectors within a third country [Article 45(1)]. In addition to being procedurally easier to achieve, an adequacy regime tailored to data concerning health could support improved responses to new challenges in healthcare, an ecosystem in which there is already substantial convergence in values and approaches.[58] Moreover, the adoption of a normative definition of 'transfers of data concerning health' could help to determine the data sharing arrangements, (remote) access techniques and repository spaces that would be covered by a sector-specific adequacy regime.[59] However, despite its promise, discussions on adequacy in the context of health and genomics seem to have been incoherent, or even biased, in the past.[60] The rationale and bases for the Commission's decisions

[55] European Commission, Commission Staff Working Document accompanying the document 'Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, COM/2020/264 final', SWD(2020) 115 final (hereafter: Commission Staff Working Document SWD(2020) 115 final).

[56] C. Bennett and S. Oduro-Marfo, *supra* note 17, at 886.

[57] G. G. Fuster, 'Un-Mapping Personal Data Transfers', 2(2) *European Data Protection Law Review* 2016, 160-168, at 162.

[58] L. Bradford *et al*., *supra* note 23, at 23.

[59] See L. Drechsler, 'International Transfer of Health Data Cross-Sectoral Roundtable – Summary Report', *Federation of European Academies of Medicine (FEAM) European Biomedical Policy Forum* (16 October 2020), at 4, available at <https://www.feam.eu/wp-content/uploads/ITHD-Summary-report-5-Nov-2020-FINAL.pdf>; T. Mulder and M. Tudorica, 'The GDPR Transfer Regime and Modern Technologies', 19 *University of Groningen Faculty of Law Research Paper* 2020, at 5-7.

[60] See J. Stoddart *et al*., *supra* note 12, at 147-149.

to grant or deny adequacy should become more transparent and predictable in order to reduce the lack of understanding both in the EU and in third countries.[61] In this respect, it is important to bear in mind that it seems illusionary to assert unilaterally EU legal standards (and underlying bureaucratic mechanisms) globally ('Brussels effect').[62] Calls for digital sovereignty, the emergence of a "Eurocentric" approach to data governance and the creation of a European Health Data Space could hamper efforts to approximate the privacy and data protection laws of third countries with EU law.[63] Moreover, it would be advisable to avoid a situation whereby the supervisory body of a third country, tasked with monitoring the processing of data concerning health originating from the EU/EEA, was asked to treat data concerning the health of EU/EEA citizens differently from personal data of the citizens of the third country itself.[64]

5.2. **Transfers subject to appropriate safeguards provided by the controller or processor specific to transfers of data concerning health**

Article 46(2) of the GDPR sets out other legal avenues that may be relied upon by the controller to provide appropriate safeguards for transfers of data concerning health (on the condition that enforceable data subject rights and effective legal remedies for data subjects are available). These transfer tools are the following:

"(a) a legally binding and enforceable instrument between public authorities or bodies;
(b) binding corporate rules …;
(c) standard data protection clauses adopted by the Commission …;
(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission …;
(e) an approved code of conduct pursuant to Article 40 …; or
(f) an approved certification mechanism pursuant to Article 42."

5.2.1. *International legal instruments*

The GDPR allows appropriate safeguards to be ensured for transfers of personal data (concerning health) on the bases of international agreements [Article 46(2)(a)] or administrative arrangements [Article 46(3)(b)] between public

[61] C. Pauletto, 'Options towards a global standard for the protection of individuals with regard to the processing of personal data', 40(105433) *Computer Law & Security Review* 2021, at 14.
[62] C. Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems', 18(4) *German Law Journal* 2017, 881-918, at 917.
[63] See F. Naftalski, *What are the main trends in regulatory responses to Schrems II*, Ernst & Young (31 March 2021), available at <https://www.ey.com/en_gl/law/regulatory-response-trends-to-schrems-ll-decision>.
[64] Cf. R. H. Weber, *supra* note 11, at 124; J. Reichel, 'Oversight of EU medical data transfers – an administrative law perspective on cross-border biomedical research administration', 7 *Health and Technology* 2017, 389-400, at 398.

authorities or bodies. While both instruments must guarantee the same outcome in terms of appropriate safeguards, including the availability of enforceable data subject rights and of effective legal remedies, they differ in their legal nature and their adoption procedure. Unlike international agreements, which create binding obligations under international law, administrative arrangements (e.g. a memorandum of understanding) are generally not binding and, therefore, require *ex ante* authorisation by the competent supervisory authority (typically the national data protection authority).[65]

Considering that transfers of data concerning health, particularly those relating to scientific research purposes, are unique forms of international data transfers (usually subject to separate legal and ethical conditions), the conclusion of bilateral or multilateral agreements or administrative arrangements outlining principles governing international health data transfers could insulate them from problematic jurisdictional conflicts.[66] The scope and content of these normative instruments could be tailored to specific purposes (e.g. the needs and functions of scientific research), which would reduce the legal uncertainty. In order to respond to technological developments and to support innovation, these normative instruments should not only cover transfers of data concerning health and their protection, but should also recognise and protect the free movement and value of the proprietary algorithms of underlying new health information technologies.[67] In addition, an international organisation (e.g. a specialised UN agency, practically: the World Health Organization) could be delegated to administer the implementation of these normative instruments, attempting to harmonise critical points of divergences and helping to settle any disputes.[68]

5.2.2. *Binding corporate rules*

The use of binding corporate rules (BCR), approved by the competent supervisory authority, permits transfers of personal data between the various undertakings of a multi-jurisdictional corporate group. Although BCR constitute a possible legal avenue, they are not yet of great significance in the context of healthcare. However, since there is a gradual uptake of IoT-enabled solutions for monitoring the health and well-being of employees, BCR may well become more relevant in future.

5.2.3. *Standard data protection clauses*

The most widely used transfer tool under Article 46 of the GDPR is standard data protection clauses, i.e. standard (model) contractual clauses (SCC) incor-

[65] Commission Staff Working Document SWD(2020) 115 final, *supra* note 55, at section 7.2.

[66] D. Hallinan *et al*., *supra* note 30, at 5-6.

[67] See World Economic Forum, *supra* note 9, at 38.

[68] Cf. P. De Hert and V. Papakonstantinou, 'Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?', 9 *I/S: A Journal of Law and Policy for the Information Society* 2013, 271-324, at 321-322; ALLEA *et al*., 'International Sharing of Personal Health Data for Research' (April 2021), at 35, available at <www.doi.org/10.26356/IHDT>.

porated voluntarily by the data exporter and the data importer into their contractual arrangements, establishing requirements for the implementation of appropriate safeguards.[69] Although SCC were originally designed to be bilateral contractual agreements, this does not exclude the possibility of incorporating them into multilateral agreements between the parties of a consortium.[70] Although they are broadly used, SCC are often considered inflexible, particularly for transfers of data concerning health. Given that SCC cover all types of personal data transfers, they contain either too onerous or too vague terms for health-related purposes and may even be in conflict with the laws of third countries.[71] By adding clarifications, however, there is a risk that SCC may be undermined or their spirit contradicted, thereby eliminating the desired legal justification for transfers of data concerning health.[72] SCC should be adapted to permit more flexibility in reflecting the specific circumstances and relationships between the parties.[73] In this regard, the revised Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries[74] seems to provide more adjustability to cover new data transfer scenarios and more complex processing operations.[75] However, it remains to be seen whether data protection safeguards enshrined in these SCC will operate consistently with the legal concepts introduced by the Data Governance Act.[76]

5.2.4. *Codes of conduct and certification mechanisms*

Stakeholders are keen to develop two further data transfer mechanisms under the GDPR: codes of conduct [Article 46(2)(e) pursuant to Article 40] and certification mechanisms [Article 46(2)(f) pursuant to Article 42].[77] Both instruments are bottom-up tools (and may be part of a middle-out approach) allowing for tailor-made solutions which reflect, for instance, the specific features and needs

---

[69] Commission Staff Working Document SWD(2020) 115 final, *supra* note 55, at section 7.2.

[70] P. Kosseim *et al*., 'Building a data sharing model for global genomic research', 15 *Genome Biology* 2014, at 4.

[71] L. Bradford *et al*., *supra* note 23, at 8-9.

[72] M. Phillips, *supra* note 14, at 580.

[73] Multistakeholder expert group to support the application of Regulation (EU) 2016/679, *Contribution from the Multistakeholder expert group to the Commission: 2020 Evaluation of the General Data Protection Regulation*, Report (17 June 2020), at 26, available at <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=41708>.

[74] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, C/2021/3972, *OJ* [2021] L 199/31, 7.6.2021.

[75] European Data Protection Board and European Data Protection Supervisor, Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries for the matters referred to in Article 46(2)(c) of Regulation (EU) 2016 (14 January 2021), at 7 (para. 18).

[76] Cf. European Data Protection Board, Statement 05/2021 on the Data Governance Act in light of the legislative developments (19 May 2021), at 1-5.

[77] See Multistakeholder expert group to support the application of Regulation (EU) 2016/679, *supra* note 73, 37.

of the health sector or health data flows. Their scope of subjects may also include controllers and processors located in third countries, and involve accredited bodies providing assurance outside the EU/EEA on conformity with the criteria established by these instruments. Certification mechanisms are flexible, scalable and provide upfront assurance, but it can be challenging to reach agreements on framework rules, to pass the rigorous upfront scrutiny needed to gain entry, and to determine which bodies qualify as legitimate third party certifiers.[78] ISO 27701 (the Personal Information Management Systems extension to the ISO 27001 Information Security Management System) has been proposed as a possible GDPR certification mechanism that could be of relevance in this context.[79] From an organisational perspective, the APEC CBPR provides an example of how oversight mechanisms can be established (although its relationship between the normative criteria and redress mechanisms does not fully correspond to the conditions of certification mechanisms established in the GDPR).[80]

In comparison with certification mechanisms, codes of conduct are more cost-effective and better suited to controllers/processors performing a particular sector-specific activity.[81] The advantage of having a sector-based code of conduct in the healthcare industry (covering transfers of data concerning health) is that it would be accessible to all organisational stakeholders in the health data ecosystem, regardless of the resources available to them.[82] Although the EDPB has adopted guidelines to foster their use, work is still ongoing to develop criteria to approve them as international data transfer tools. Current initiatives for codes of conducts, which could be of relevance in this context, are still in their preparatory phases or have not been approved. To ensure its universal application and accountability, a code of conduct covering international transfers of data concerning health could be positioned within the human rights framework and could support the implementation of the right to benefit from scientific progress and its applications.[83]

5.3. **Supplementary measures specific to transfers of data concerning health in addition to appropriate safeguards provided by the controller or processor**

If the data exporter's assessment reveals that its Article 46 GDPR transfer tool is not effective, then it will need to consider (if appropriate, in collaboration with

[78] P. Kosseim *et al*., *supra* note 70, 4-5.

[79] C. Compagnucci *et al*., 'Lost on the High Seas without a Safe Harbor or a Shield? Navigating Cross-Border Data Transfers in the Pharmaceutical Sector After Schrems II Invalidation of the EU-US Privacy Shield', 4 *European Pharmaceutical Law Review* 2020, 153-160, at 46.

[80] I. Kamara *et al*., *Data Protection Certification Mechanisms, Study on Articles 42 and 43 of the Regulation (EU) 2016/679*, Final Report (Luxembourg: Publications Office of the European Union 2019), at 214-216.

[81] Commission Staff Working Document SWD(2020) 115 final, *supra* note 59, at section 7.2.

[82] See D. D. Hirsch, 'In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct', 74 *Ohio State Law Journal* 2013, 1029-1069, at 1053-1054.

[83] B. M. Knoppers *et al*., 'A human rights approach to an international code of conduct for genomic and clinical data sharing', 133 *Human Genetics* 2014, 895-903, at 898-901

the data importer) whether supplementary measures exist, which, when added to safeguards embodied in transfer tools, can ensure that the transferred data is afforded a level of protection in the third country essentially equivalent to that guaranteed within the EU/EEA. The data exporter must identify on a case-by-case basis the supplementary measures that could be effective for data transfer to a third country when using a specific Article 46 GDPR legal avenue.[84] In principle, supplementary measures may have a technical, additional contractual or organisational nature.[85] The combination of these different measures can enhance the level of protection, and may therefore contribute to reaching the level of EU data protection standards.[86]

5.3.1. *Technical measures*

Technical measures are intended to ensure that access to the transferred data by public authorities in third countries does not impinge on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools.[87] In this respect, the following solutions are considered effective supplementary measures for the protection of data concerning health:[88]

- state-of-the-art encryption of data storage for backup purposes that does not provide access to unencrypted data concerning health;
- transfer of pseudonymised data (concerning health) with appropriate technical and organisational safeguards;
- data concerning health merely transiting through third countries;
- a data exporter transfers data concerning health using state-of-the-art encryption to a data importer in a third country, whose law exempts the data importer from potentially infringing access to the data, e.g. by virtue of professional/medical secrecy; or
- split or multi-party processing, i.e. prior to transmission, the data exporter splits personal data (concerning health) in a way that does not allow individual processors (acting as data importers) to receive sufficient amounts of data to reconstruct the personal data (concerning health) in whole or in part.

It is important to emphasise that cases where unencrypted data concerning health are technically necessary for the provision of a service, such as transfers of data concerning health to third country cloud service providers or other processors, which require access to such data, do not qualify as appropriate supplementary measures.[89] In these scenarios, there is a risk of 'data mingling', i.e. data concerning health may mix with other data, and cloud processors might

[84] EDPB Recommendations 01/2020 (*supra* note 32), at 15 (para. 46).
[85] Ibid., at 15 (para. 47).
[86] Ibid.
[87] Ibid., at 21-22 (para. 74).
[88] See ibid., at 22-26 (para. 79-86).
[89] See ibid., at 26-27 (para. 88-89).

actively 'mine' data concerning health to gain intelligence for commercial gains.[90] It is also worth noting that there are technical measures that do not involve actual transfers of data concerning health, such as remote access to data via a thin client (data visitation) or by remote execution.[91] To counter the misuse of techniques by which extra-jurisdictional insights into data concerning health might be obtained (without the data leaving the local server), the locally stored data concerning health can be tagged/referenced.[92] The data tag/reference is suitable to make a request to the data repository in the receiving country, and each of those requests can be authorised by the data exporter.[93]

Alternatively, distributed ledger technologies (DLT) can be implemented, given that they can help to document the origin and complete historical record of data in an immutable or tamper-evident record. In this case, every instance of data transfer or other form of data processing becomes traceable. DLT have been proposed as a solution for structuring the system rules (transactions, governance and operations) of transborder data networks in the post-*Schrems II* environment.[94] DLT could be deployed to provide an ecosystem in which individuals can maintain ownership of their data concerning health (personal electronic health records) and decide how to share their data and under what conditions.[95] DLT solutions could provide opportunities to automate the data access control procedure and improve transparency and fairness in accessing data concerning health, while the enforceability of access agreements could be improved by using DLT-based smart contracts.[96]

5.3.2. *Additional contractual measures*

Additional contractual measures may complement and reinforce the safeguards provided by the transfer tool and the legislation of the third country, when these do not meet all the conditions required to ensure a level of protection essentially equivalent to that guaranteed within the EU/EEA.[97] Possible additional contractual measures may include:[98]

---

[90] J. J. M. Seddon and L. W. Currie, 'Cloud computing and trans-border health data: Unpacking U.S. and EU healthcare regulation and compliance', 2 *Health Policy and Technology* 2013, 229-241, at 233-234.

[91] See D. Hallinan *et al*., *supra* note 30, at 5.

[92] World Economic Forum, supra note 9, at 38.

[93] Ibid.

[94] E. Renieris and D. Greenwood, 'Unblocking blockchain data flows in the wake of *Schrems II*', *MIT Computational Law Report* (14 August 2020), at 7, available at <https://law.mit.edu/pub/unblockingblockchaindataflowsinthewakeofschremsii/release/1>.

[95] A. Dubovitskaya *et al*., 'Applications of Blockchain Technology for Data-Sharing in Oncology: Results from a Systematic Literature Review', 98 *Oncology and Informatics – Review* 2020, 403-411, at 404.

[96] M. Shabani, 'Blockchain-based platforms for genomic data sharing: a de-centralized approach in response to the governance problems?', 26 *Journal of the American Medical Informatics Association* 2019, 76-80, at 79.

[97] EDPB Recommendations 01/2020 (*supra* note 32), at 28 (para. 93).

[98] Ibid, at 29-34 (paras. 99-121).

- obligation of both parties to use specific technical measures;
- transparency obligations of the data importer (which could include the power of the data exporter to conduct audits and the obligation of the data importer to inform the data exporter promptly of its inability to comply with the contractual commitments); or
- *ad hoc* redress mechanisms to empower data subjects to exercise their rights.

In order to enhance the transparency and accountability of contractual arrangements, the legal responsibilities of those involved should be clarified once the data transfer takes place.[99] According to one argument, data exporters should remain liable under most circumstances for data protection breaches caused by data importers, as the data exporter is likely to be the entity that is more easily accessible for the data subject.[100] On the other side, data importers should demonstrate their capacity to provide assurances that adequate protection mechanisms are in place.[101]

5.3.3. *Additional organisational measures*

Additional organisational measures may help to ensure consistency in the protection of data concerning health during the full data processing cycle. These measures may consist of internal policies, organisational methods and standards that data exporters can apply and impose on data importers in third countries.[102] Possible organisational measures may include:

- clear allocation of responsibility for transfers of data concerning health (e.g. appointment of a project team);
- data access and confidentiality policies and best practices, based on data minimisation measures and a strict 'need-to-know' principle, monitored by regular audits; or
- timely involvement of the Data Protection Officer and Internal Audit Department.

In the case of international health research collaborations, research ethics committees play a pivotal role (in combination with national supervisory bodies) in ensuring that 'appropriate safeguards' are in place before the launch of cross-jurisdictional projects.[103] From an inter-organisational perspective, international health data trusts or a network of national health data trusts residing in different jurisdictions could act as data intermediaries by managing data con-

---

[99] See F. Molnár-Gábor, 'Germany: a fair balance between scientific freedom and data subjects' rights?', 137 *Human Genetics* 2018, 619-626, at 626.

[100] World Economic Forum, *supra* note 9, at 29.

[101] J. Alhadeff *et al*., 'The Accountability Principle Data Protection Regulation: Origin, Development and Future Directions', in D. Guagnin *et al*. (eds.), *Managing Privacy through Accountability* (Basingstoke: Palgrave Macmillan, 2012), 49-82, at 68-69.

[102] Ibid., at 35 (para. 122).

[103] J. Reichel, *supra* note 63, at 391, 399.

cerning health on behalf of data suppliers in a federated health data ecosystem.[104]

5.4. **Derogations for specific situations in the healthcare sector**

If neither an adequacy decision nor any other transfer tool is available, then transfers of data concerning health outside the EU/EEA may be performed based on one of the 'specific situation' grounds outlined in Article 49 of the GDPR. The legal justifications (derogations), which are mostly relevant in the health-related domain are the following:

> "(a) the data subject has explicitly consented to the proposed transfer …;
> (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; […]
> (d) the transfer is necessary for important reasons of public interest; […]
> (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent".

These derogations must be interpreted restrictively.[105] As derogations do not provide adequate protection or appropriate safeguards for data concerning health, these avenues carry increased risks for the rights of the data subject concerned.[106] Although the explicit and specific consent of the data subject for a particular (set of) transfer(s), after having been informed of the possible risks of such transfers, may be considered a valid legal ground, the EDPB has reiterated that even in this case, data transfers occurring periodically or under random circumstances and within arbitrary time intervals are inappropriate.[107] This narrow interpretation of consent should be borne in mind, in particular, by developers and operators of IoT-enabled telehealth systems that are dependent on transborder data flows. In other situations, the data exporter must perform a necessity test to evaluate whether the transfer of data concerning health is necessary for the specific purpose of a derogation.[108] For example, if a contract exists between a health app service provider and a user, the controller must be able to demonstrate that the transfer of data concerning health outside the EU/EEA has a close and substantial link to the main purpose of the contract.[109] In the event of medical emergency, or when the data subject does not have the physical, mental or legal ability to make a valid decision, the transfer of data concerning health must be necessary for the purpose of an essential diagnosis.[110]

---

[104] See World Economic Forum, *supra* note 9, at 39-40.

[105] European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (25 May 2018) (hereafter: EDPB Guidelines 2/2018), at 4.

[106] See ibid.

[107] Cf. ibid., at 4-8; European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1 (4 May 2020), at 20 (footnote 47).

[108] EDPB Guidelines 2/2018, *supra* note 105, at 5.

[109] L. Bradford *et al*., *supra* note 23, at 9.

[110] EDPB Guidelines 2/2018, *supra* note 105, at 12-13.

The EDPB considers that the fight against COVID-19 has been recognised by the EU and its Member States as an 'important public interest', "which may require urgent action in the field of scientific research (for example to identify treatments or develop vaccines), and may also involve transfers to third countries or international organisations."[111] The EDPB has stated that:

> "[p]ublic authorities and private entities may, under the current pandemic context … rely upon the applicable derogations mentioned above, mainly as a temporary measure due to the urgency of the medical situation globally. […] Indeed, if the nature of the COVID-19 crisis may justify the use of the applicable derogations for initial transfers carried out for the purpose of research in this context, repetitive transfers of data to third countries part of a long lasting research project in this regard would need to be framed with appropriate safeguards in accordance with Article 46 GDPR."[112]

This guideline has been criticised due to its lack of urgency with regard to the consideration that epidemiological research requires access to data over time to conduct longitudinal studies; a 'temporary measure' does not suffice in the long-term.[113] For this reason, the list of 'derogations for specific situations' could be expanded to include a legal avenue for cases when 'transfer is necessary for scientific research in an epidemiological context' subject to appropriate supplementary measures.[114]

6. CONCLUSION

The COVID-19 crisis and the CJEU's *Schrems II* judgment have intensified the data protection challenges for entities involved in transfers of data concerning health from the EU/EEA to third countries. By analysing the underlying policy considerations and the implications of *Schrems II* and its impact on subsequent case law and authoritative legal interpretations, this paper argues that the adoption of legal avenues and the implementation of supplementary measures tailored to the specificities of the healthcare sector would reduce barriers and facilitate transfers of data concerning health. Considering that data concerning health generally enjoy distinct normative treatment, this paper proposes the adoption of sector-specific international legal instruments, adequacy decisions, codes of conduct, certification mechanisms and a specific derogation for scientific research in healthcare. In addition to appropriate safeguards provided by the controller or processor, the effective deployment of technical, contractual and organisational measures can ensure that the level of protection afforded to data concerning health in a third country is essentially equivalent to that guaranteed within the EU/EEA.

---

[111] European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (21 April 2020), at 12-13 (para. 63).

[112] Ibid., at 13 (paras. 66-67).

[113] See J. Bovenberg *et al.*, *supra* note 27, at 41.

[114] Ibid., at 42.