The Application of GDPR to Biomedical Research: Stakeholder Advisory Opinions to Assist Regulators

Prepared for the ISC Seminar on Challenges for Health Research Arising from the GDPR

19 November 2019

Brussels, Belgium

TABLE OF CONTENTS

Page

The Application of GDPR to Biomedical Research: Stakeholder Advisory Opinions to Assist Regulators [1]

I. Introduction

Over the past decade, research has become increasingly international, with both interventional and secondary research studies often spanning national borders. At the same time, the growth of "big data" and the advancement of analytic technologies has meant that the ability to analyze existing data sets for research purposes and to share datasets across national borders as part of research collaborations has taken on increased importance. This desire for greater access to, and use of data for, research purposes has introduced a certain tension between protecting the privacy of individuals whose data are shared and facilitating important research projects. Legislators, public health officials, and scientists around the world are currently grappling with this issue and seeking to strike a balance between the privacy interest of individuals and the public interest in research.[2]

As a law of general and multi-sectoral applicability with a broad extraterritorial scope, the General Data Protection Regulation ("GDPR") has reached and affected research uses of personal data within the European Union ("EU")[3] and beyond, including research in leading centers of research, such as the United States, South Africa, and Switzerland.

The research community followed with great interest and appreciated the extensive attention paid by the EU government to research issues during the drafting and negotiation of GDPR, which has resulted in several provisions of GDPR that may facilitate the processing of personal data for scientific research. We highlight the following provisions in particular:

- GDPR provides as an exception to the general prohibition on the processing of "special categories" of personal data, the processing of such data for scientific and historical research purposes based on European Union or member state law, provided appropriate conditions and safeguards are in place to protect the rights and freedoms of data subjects;[4]

- GDPR explicitly exempts research from the compatibility element of the purpose limitation principle and from the storage limitation principle, if certain conditions are met. These exemptions are specifically welcome, as they provide researchers with the leeway

---

[1] This paper was prepared by the Multi-Regional Clinical Trials Center of Harvard University and Brigham and Women's Hospital (MRCT Center), Ropes & Gray LLP (Mark Barnes, JD, LL.M., David Peloquin, JD and Nicholas Wallace, JD) as a *pro bono* service to the MRCT Center, and Jasper Bovenberg, JD, LL.M., Attorney at law licensed to practice in the Netherlands and New York, Certified International Privacy Manager, Certified International Privacy Professional, Founder & CEO of the Legal Pathways Institute for Life Science Law. The authors wish to thank Barbara Bierer, MD, Robert Eiss, MA, Declan Kirrane, Maryline Maillard, MA, Triona McCormack, and Kurt Zatloukal, MD, for their comments on, and contributions to, this paper.

[2] Recent years have seen the adoption of new, comprehensive privacy legislation in several countries worldwide, including Brazil's General Data Protection Law, which takes effect in August 2020, Japan's Act on Protection of Personal Information, to which substantial amendments took effect in May 2017, and, in the United States, the introduction of privacy legislation at the state level, including most notably the California Consumer Privacy Act, which takes effect on January 1, 2020.

[3] In this paper, for ease of reference, we use the term "EU" to refer to the EU, its member states, and the three additional states that, together with the EU member states, comprise the European Economic Area—Norway, Iceland, and Liechtenstein.

[4] *See* GDPR, art. 9(2)(j).

to store data and repurpose it for research, which is expedient to conducting artificial intelligence ("AI") and "big data" research on health data;[5]

- GDPR's principle that processing personal data for scientific or historical research is not incompatible with the initial purposes can be read to permit such processing without a separate legal basis from that which permitted the initial processing.[6] The allowed subsequent research is not limited to any specific research project but applies to scientific and historical research in general;

- GDPR's recitals explicitly allow data subjects to give general consent rather than specific consent for processing for research purposes in circumstances in which it is not possible to identify fully the purpose of personal data processing at the time of initial data collection, and provided data subjects are offered the option to give specific consent;[7]

- GDPR exempts from the right of erasure personal data processed for scientific research purposes if erasure is likely to render impossible or seriously impair the achievement of the objectives of the processing;[8]

- GDPR explicitly recognizes registries as an important means of scientific research;[9] and

- GDPR permits member states to enact derogations from various data subject rights in the research context if the exercise of such rights would render impossible, or seriously impair, the research process.[10]

In these ways, based on a straightforward, "plain meaning" reading of GDPR's text, it would appear as though there should be few problems with applying GDPR to allow important scientific and medical research to continue. However, unfortunately, in spite of these many apparently research-friendly provisions of GDPR, there has to date not been any official guidance tying together these various, disparate GDPR provisions into a cohesive pathway to facilitate research. The trend in practice has been the opposite, as regulators, ethics committees, and institutions have taken disparate positions leading to a patchwork of requirements for multi-country research studies. Certain of these interpretations are contrary to decades of established practice in the research community and foundational principles of research ethics. These interpretations have also frustrated the purpose articulated in GDPR recital 159, which notes the need to "take into account the Union's objective under Article 179(1) [of the Treaty on the Functioning of the European Union] of achieving a European Research Area."

Some have opined that in regard to research, GDPR has not essentially changed the requirements of the 1995 Data Protection Directive (Directive 95/46/EC) (the "Data Directive"), and the research community should therefore just learn to comply with GDPR, as it learned to comply with the Data Directive. We think this point of view misunderstands the many challenges that GDPR has introduced for the research community that were not present under the Data Directive. First, the requirements under GDPR – and especially under the interpretive guidance offered to date – as applied to research with human data are more specific than any guidance that

[5] *See* GDPR, art. 5(1)(b), (e).
[6] *See* GDPR, art. 5(1)(b), recital 50.
[7] *See* GDPR, recital 33.
[8] *See* GDPR, art. 17(3)(d).
[9] *See* GDPR, recital 157.
[10] *See* GDPR, art. 89(2).

was issued under the Data Directive. Second, specific points – such as the acceptable use in clinical trials of consent as a basis for processing of personal data under the Data Directive, have now been altered through GDPR guidance, even if the terms of GDPR itself could be compatible with previous approaches to compliance under the Data Directive. Third, GDPR comes with substantial penalties for non-compliance, far exceeding any set forth in member state legislation issued under the Data Directive, thus making the entire research community extremely hesitant to engage in data practices not sanctioned explicitly by guidance, for fear of penalties. Fourth, this reluctance even to engage in data practices that appear acceptable under a plain reading of GDPR is made more acute by the ways in which official guidance interpreting GDPR seems to vary from GDPR's text. As a matter of regulatory compliance behavior of civil society, it should surprise no one that increased penalties, more specific requirements, and official guidance that appears to contradict GDPR's text might result in reluctance to act, or even a kind of compliance paralysis. If the only effect of this uncertainty were to delay or deter commercial or market research, then this might be tolerable; but the effect instead is to delay or defer crucial scientific and clinical research that is necessary to improve health and wellness, which is contrary to personal and social interests throughout the EU.

We are aware and appreciative of a number of initiatives undertaken to help researchers prepare for the implementation of GDPR, notably in the area of health research (dedicated meetings with stakeholders, the Commission's general guidance[11], and a practical online tool[12]). We are also aware and appreciative that the challenges described above have not escaped the attention of the Commission and the member states, as they have prepared a set of questions for request to issue guidelines for the consistent application of GDPR in health research focusing on international relations and trans-national cooperation. In addition, the European Parliamentary Research Service has prepared a study paper examining how GDPR changes the rules for scientific research.[13]

This paper is the result of several months of conversation among an international coalition of stakeholders interested in the effect of GDPR on scientific research, which includes representatives from Austria, Belgium, Ireland, the Netherlands, South Africa, Switzerland and the United States. This group initially came together in July 2018 at a conference of the Multi-Regional Clinical Trials Center of Harvard University and Brigham and Women's Hospital, which was followed by a meeting with the Irish Data Protection Commission in Dublin in May 2019, and the organization of the present seminar in Brussels in November 2019. To provide input and add perspective to this effort, as well as to underscore the urgency of the issues raised, we have prepared this paper, which begins by providing case studies of actual research endeavors that have been interrupted, halted, or reduced in scientific merit as a result of certain interpretations of GDPR. Next, the paper summarizes the legal issues under GDPR and the interpretive guidance that has led to this disruption of longstanding research relationships. Finally, this paper proposes changes to GDPR's implementing guidance that would continue to protect personal data of data subjects while allowing valuable research endeavors to proceed.

[11] COM(2018) 43 final Commission Communication 'Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018

[12] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en

[13] *See, e.g.*, European Parliamentary Research Service, *How the General Data Protection Regulation changes the rules for scientific research* (July 2019), http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)634447.

We note that because GDPR has an expansive extra-territorial jurisdiction, the issues discussed in this paper affect researchers not only in the EU, but located throughout the world. The issues discussed below in Sections II.A-E apply equally to research studies that take place within the EU and those that take place outside of the EU, because they arise whenever the processing of personal data for research purposes is subject to GDPR. The issues discussed in Section II.F-G apply whenever a research study involves the transfer of personal data from an EU member state to a country located outside of the EU (or "third country," to use the language of GDPR) that lacks an "adequacy decision" from the European Commission. These issues thus arise in the vast majority of multi-national research studies involving EU member states and third countries, because only a handful of third countries have to date received adequacy decisions.[14]

It is hoped that this paper will make cognizant authorities aware of the adverse consequences that result from confusing interpretations of GDPR as applied to processing of personal data for research purposes and the research community's consequent reluctance to embrace fully the specific provisions of GDPR that could otherwise facilitate research. For each challenge identified, we suggest possible solutions that will permit the potential of GDPR's research provisions to be realized.

II. Case Studies

The following examples are important because they demonstrate the ways in which GDPR has, and will predictably continue to, interrupt research that long has been recognized as socially and ethically desirable. The research affected by GDPR includes both projects conducted wholly within the EU and projects that involve the EU and third countries. As we describe in the following Section II, there are, however, alternatives for GDPR to be applied through regulatory approaches that are protective of data subjects and are more consistent with good science and public health.

First, we are aware of a number of examples in which international research studies and collaborations have been impeded by certain elements of GDPR's restrictions on international data flows, both into and out of the EU.

- *University College Dublin has adapted to GDPR by splitting certain multi-national research studies into two studies, one in the EU and one outside of the EU, solely to comply with GDPR's restrictions on transfers of personal data to third countries.* Using this approach, the researchers cause to be maintained two separate data sets and conduct a meta-analysis separately in each location, transferring only the meta-analysis from the non-EU countries to the EU and vice versa. Practices such as this, contrived to achieve legal compliance but not based on scientific need, are suboptimal because they can have an adverse impact on the statistical analysis, the number of participants required, and the comparability of the two data sets. Additionally, such practices have increased the costs of conducting the research and, most importantly, have constrained research teams from having a global picture of the research data that would allow them to conduct the most productive analyses to advance science. Such approaches also introduce risk of

[14]The only countries with an adequacy decision are Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework, which is available only to for-profit organizations).

inaccuracy and mistake, because a data processing step has been implemented due to legal compliance considerations, having nothing to do with scientific method.

- *The International Genomics of Alzheimer's Consortium and the U.S.-based Alzheimer's Disease Sequencing Project based at the University of Pennsylvania Perelman School of Medicine have been unable to pool personal data on a single server for streamlined processing because EU investigators have indicated that they believe that due to GDPR they cannot share the European personal data with U.S.-based researchers.* This creates a scientifically compromised, inefficient, and more expensive distributed analysis of international Alzheimer's Disease data in the search for novel drug targets, because investigators must run identical analyses on segregated pools of data in different locations. In terms of scientific compromise, the distributive analysis model that EU researchers and their global collaborators have been forced to adopt both slows research and limits the scope of research projects in which they can engage—it is anticipated that the bifurcation of the data sets will add a full year to the completion of a study that is in progress and will also limit the number of different projects that can be performed using the data.

- *As a transplant center pursuing both research and patient care, the U.S. National Institutes of Health Unrelated Donor Hematopoietic Stem Cell Transplant Program recruits the most favorable stem cell donors they can identify for its patients.* Around 40% of its unrelated donors reside in Europe. Donor samples are obtained through the National Marrow Donor Program ("NMDP") partnerships with a network of donor centers in Germany, Norway, Poland, Sweden, and the United Kingdom. When there is a match and NIH requests a sample, the NMDP or its international collaborator contacts the donor, obtains informed consent, and collects the sample. In May 2018, the German donor center ("DKMS") requested that NIH comply with GDPR, prior to receiving additional samples for research purposes. Because the United States does not have an adequacy determination and because NIH cannot sign the standard contractual clauses, NIH proposed obtaining explicit consent from donors for the transfer of their sample to the United States. DKMS rejected this option, stating that transfers based on explicit consent are "only permissible in exceptional cases." The inability of NIH to now make use of German or other European donors for patients on these protocols, excludes these patients from immunotherapy and other treatment. In a recent case, NIH was in process of working with the NMDP to request an exception from the DKMS, but the delay caused by GDPR resulted in the patient's becoming too ill to proceed under the protocol. The experience highlights that GDPR is not just a data issue per se, but has direct effects on patient care.

Second, intra-EU divergences in member state authorities' interpretation of GDPR have led to impediments conducting research even across EU countries—an especially disheartening result given that GDPR was intended to bring uniformity to the regulation of personal data processing throughout the EU. For example, as described in greater detail in the analysis below, different EU regulatory authorities have taken divergent positions with respect to whether consent may be the basis for processing personal data in the context of a research study.

Third, the EU member states have not yet finalized efficient processes for permitting the approval of bespoke data transfer clauses or determining that data may be transferred under other derogations, such as the derogation permitting data to be transferred when necessary for

important reasons of public interest, which has led to the delay of important research involving non-EU governmental entities that are unable to sign standard contractual clauses.

- The Finnish National Institute of Health and Welfare ("THL") and the NIH's National Human Genome Research Institute ("NHGRI") have been engaged in an ongoing 25-year diabetes genetics research study for which NIH director Dr. Francis Collins serves as a principal investigator. The study represents a leading source of continuing knowledge on genetic determinants of Type 2 diabetes. To date, the collaboration has identified over 80 genetic susceptibility loci for Type 2 diabetes. As discussed in further detail below, the NIH is unable to sign the standard contractual clauses to permit the transfer of personal data from the EU to the U.S., and thus data transfer from Finland to the U.S. for this project largely ceased on May 25, 2018. THL and NHGRI negotiated bespoke data transfer clauses that were submitted to the Finnish data protection authority for approval. While awaiting a decision, and 16 months after the effective date of GDPR, the general counsel of THL determined that data transfers could in fact resume under GDPR's derogation to the prohibition on international data transfers for transfers that are "necessary for important reasons of public interest." While this very recent determination has been extremely helpful to the THL/NHGRI collaboration, the lack of clear guidance regarding when this derogation may be used for research collaborations more generally has made it difficult for the broader research community to assess the extent to which one may rely upon this basis for transfer.

Fourth, because GDPR applies to personal data that are processed in the EU even when the data originate outside the EU and pertain solely to non-EU data subjects, non-EU researchers have found their non-EU projects affected by GDPR when they choose to use vendors located in the EU, such as central laboratories and data analysis companies. This has caused non-EU controllers to take, in many instances, a second look at whether using a vendor in the EU is worth the cost of negotiating required data protection clauses when neither the controller nor the data are subject to GDPR in the first instance, meaning that GDPR would not apply to the study but for the use of a vendor located in the EU. This state of affairs has caused EU data processors, such as clinical research support and data analysis companies, to be at a competitive disadvantage vis-a-vis their non-EU counterparts. This may be a cost that the EU member states are willing to endure in the pursuit of ensuring privacy protections even for non-EU residents, but that this cost is being incurred is at least worthy of note.

III. Summary of GDPR Interpretive Issues and Proposed Solutions

A. *Difficulties in Identifying Clear Legal Basis for Processing Data for Prospective Research*

We have seen differing approaches regarding the legal basis for processing personal data for prospective research,[15] both on the part of regulators and on the part of research entities. This has introduced challenges for researchers, including both private industry researchers and university/hospital researchers. Specifically, the research community has encountered differing approaches regarding the threshold question of the appropriate legal basis for processing personal

[15]This paper uses the term "prospective research" to refer to research in which data are generated and collected from subjects expressly for the purpose of the research study in question. We use the term "secondary research" to refer to research using data that were collected in another primary or initial activity, such as clinical care, health or social services delivery, or another research study.

data and conditions for processing special categories of personal data for prospective research. Adding confusion, most biomedical research involves "special categories" of personal data (e.g., health data, genetic data) and thus requires both a basis for processing personal data under GDPR Article 6 and an exception to the prohibition on processing of special categories of personal data under GDPR Article 9. The European Data Protection Board ("EDPB") and the European Commission Directorate-General for Health and Food Safety ("EU Commission") have issued guidance on this topic, proposing that controllers conducting prospective research in the form of interventional clinical trials of a medicinal product should rely on different bases for processing personal data, depending on whether the processing is for purposes of (1) reliability and safety or (2) research activities.[16]

If processing data for reliability and safety purposes, the EDPB and EU Commission recommend relying on Article 6(1)(c), legal obligation of the controller, and Article 9(2(i), "processing necessary for reasons of public health and of medicinal products." The EDPB has referred to the Article 29 Working Party guidance, noting that "the obligation must be imposed by law; the law must fulfil all relevant conditions to make the obligation valid and binding; the law must comply with data protection law, including the requirement of necessity, proportionality and purpose limitation; the legal obligation itself must be sufficiently clear as to the processing of personal data it requires; and the controller should not have an undue degree of discretion on how to comply with the legal obligation.[17]

If processing personal data for clinical research purposes, the EDPB and European Commission disfavor reliance on consent as a basis for processing personal data, stating that consent is often not "freely given" in the context of a research study because there exists a power imbalance between the data subjects and the investigator or institution conducting the research. The EDPB elaborates that "this will be the case when a participant is not in good health conditions, when participants belong to an economically or socially disadvantaged group or in any situation of institutional or hierarchical dependency. . . consent will not be the appropriate legal basis in most cases, and other legal bases than consent must be relied upon."[18] The EDPB thus recommends reliance on processing based on a task carried out in the public interest in the area of public health (Article 9(2)(i)) or processing for scientific research purposes in accordance with Article 89(1) (Article 9(2)(j)). The EDPB also notes that the "legitimate interest" basis under Article 6(1)(f) may be available "where the conduct of clinical trials cannot be considered as necessary for the performance of the public interest tasks vested in the controller by law" and it would appear that

[16]*See* European Commission Directorate-General for Health and Food Safety, *Question and Answers on the Interplay Between the Clinical Trials Regulation and the General Data Protection Regulation*, https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf (last accessed September 18, 2019); European Data Protection Board, *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b))* (adopted Jan. 23, 2019).

[17]The EDBP guidance continues, noting that "The EDPB considers that this is notably the case for obligations relating to the performance of safety reporting under Articles 41 to 43 of the CTR, and obligations concerning the archiving of the clinical trial master file (for at least 25 years according to Article 58 CTR) and the medical files of subjects (which is to be determined by national law according to the same provision). The same applies to any disclosure of clinical trial data to the national competent authorities in the course of an inspection in accordance with relevant national rules (see Articles 77- 79 CTR)." Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CT) and the General Data Protection regulation (GDPR) (art. 70.1.b)) (Jan. 23, 2019), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf.

[18]European Data Protection Board, *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b))*, (adopted Jan. 23, 2019).

such interest would have to be coupled with Article 9(2)(j) for processing special categories of personal data.[19]

Likewise, the United Kingdom Health Research Authority ("HRA") takes the position that, while "most research studies that have involved use of confidential patient information have sought consent from participants" to "avoid a breach of the common law duty of confidentiality," GDPR requires a statutory legal basis separate from consent used to satisfy the common law duty.[20] The HRA takes the position that, under GDPR, "consent would not be appropriate as a legal basis . . . where there is an imbalance of power in the relationship between the controller and the data subject." The HRA takes the position that "the common law duty of confidentiality is not changing, so consent is still needed for people outside the care team to access and use confidential information for research."

In contrast, Ireland's Health Research Board advises researchers that consent can be a valid basis for conducting health research using personal data.[21] We also understand that in Germany and Italy, most researchers continue to rely upon consent as the basis for processing personal data based on a requirement in the German Medicinal Products Act that participants in research studies provide consent for the processing of their personal data.

The challenge posed by the bases for processing favored by the EDPB is that both processing for public interest in the area of public health and processing for scientific research purposes require that the processing be based on other express EU or member state law. Because the EU member states differ as to whether their national laws permit processing of personal data for public health or scientific research purposes, the basis for processing varies across the EU member states.[22] The variation in the basis for processing across EU member states poses challenges to research sponsors and researchers that support or conduct research spanning multiple EU member states, which is an increasingly common phenomenon given the multi-national nature of much biomedical and other research. Research sponsors affected by this variation in interpretation include both those located within the EU and those located in third countries, such as Switzerland and the United States.

Moreover, the EDPB's guidance that consent for data processing is not "freely given" in the context of a clinical trial is at odds with standard practice in research ethics, including the Declaration of Helsinki, and the EU's own Clinical Trials Regulation, both of which typically

[19] *See id.* at para. 27.

[20] *See* U.K. National Health Service Health Research Authority, *Consent in Research* (last updated Apr. 19, 2018), https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/what-law-says/consent-research/.

[21] *See* Ireland Health Research Board, *Health Research Regulations 2018 FAQ*, https://www.hrb.ie/funding/gdpr-guidance-for-researchers/health-research-regulations-2018/health-research-regulations-2018-faq/ (emphasis added) ("The processing of personal data related to clinical trials must comply with GDPR (from 25 May 2018) and the Health Research Regulations 2018 (from 8 August). Researchers are recommended to seek project specific advice in relation to data processing for health research purposes from their organisation's DPO, **including how to ensure that consent arrangements for any research projects are consistent with the conditions for consent (to be valid) set out in Article 7 of GDPR.**").

[22] *Compare* Netherlands GDPR Implementation Act, pt. 3, div. 3.1, § 24 (providing that one may process personal data for scientific, historical or statistical research purposes without consent only when asking for explicit consent is impossible or requires a disproportionate effort) *with* Estonia Personal Data Protection Act, ch. 2, § 6 (providing that personal data may be processed for scientific research, historical research, or national statistics without the consent of the data subject so long as the data are protected throughout the research through pseudonymization and provided that certain conditions are satisfied).

require obtaining the voluntary consent of research subjects before enrolling them in a clinical trial.[23] The EDPB has never explained why it believes that a research subject's consent to the processing of personal data in connection with a clinical trial cannot be freely given, whereas consent to participate in the clinical trial itself can be freely given. It is curious for the EDPB to conclude, apparently, that a research subject can consent to receive an investigational medicinal product of unknown safety and efficacy but that another basis for data processing is recommended because of concerns that consent may not be freely given.

Proposed Solutions

The best solution for research sponsors and participants would be a uniform standard regarding the appropriate basis(es) for processing personal data for research purposes across EU member states. This could be facilitated by the EDPB's issuing guidance clarifying (i) that consent can continue to be a basis for processing personal data in the context of prospective research, such as a clinical trial, and (ii) the types of EU or member state laws that may permit processing personal data on the basis of public interest in the area of public health or for scientific or historical research purposes, preferably providing specific examples of such laws.

B. *Difficulties in Identifying Clear Legal Basis for Processing Data for Secondary Research*

Secondary research has presented particular difficulties with respect to identifying the appropriate basis for processing personal data, given that consent is almost never a viable option in such research due to passage of time and the consequent dispersion of data subjects. This type of research has increased in importance in recent years given the advent of "big data" research studies and the increasing use of "real world evidence" to supplement, and in some cases replace, interventional clinical trials, according to preferences expressed by the European Medicines Agency and similar national drug regulatory agencies around the world. This has made GDPR's failure to provide a clear basis for processing personal data for such purposes particularly challenging for the research enterprise.

The text of GDPR itself suggests a pathway for processing personal data for secondary research purposes in Article 5, which states that: "Personal data shall be . . . collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes shall, in accordance with Article 89(1), not be considered incompatible with the initial purposes." The lack of guidance regarding the ability of

[23] *See* Regulation (EU) No. 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, art. 28(1)(c) ("A clinical trial may be conducted only where all of the following conditions are met: . . . the subjects, or where a subject is not able to give informed consent, his or her legally designated representative, have given informed consent . . . ."); *see also* World Medical Association, Declaration of Helsinki https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/ ("Participation by individuals capable of giving informed consent as subjects in medical research must be voluntary.").

researchers to avail themselves of this "compatibility" principle has, however, made the research community reluctant to embrace this provision of GDPR. The EDPB briefly addressed compatibility in its January 2019 guidance on the intersection of GDPR and the EU Clinical Trials Regulation, but the EDPB highlighted the need for future guidance on this question, thus increasing uncertainty for the regulated research community; the effect of this reference to future guidance has been only to sustain the research community's reluctance to rely upon "compatibility" as a basis for the processing of personal data for secondary research. Specifically, the EDPB's guidance states that "[compatibility] due to [its] horizontal and complex nature, will require specific attention and guidance from the EDPB in the future."

Another possible basis for processing personal data is Article 9(2)(j), which, as discussed in Section II.B above, permits processing "special categories" of personal data for scientific research purposes. Reliance on the scientific research basis introduces, however, the issues discussed in Section II.B above with respect to a lack of clarity regarding which EU and/or member state laws do or might permit reliance on this basis for processing.

There have also persisted ambiguities surrounding the availability of "broad consent," that is, the ability of researchers to obtain consent from data subjects to the use of their personal data for future research studies. GDPR itself contains text that favors the use of broad consent, recognizing in Recital 33 that, "[i]t is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research. . . ."[24] The Article 29 Working Party's guidance on consent took a narrow view with respect to the application of this recital, noting that "Recital 33 does not disapply the obligations with regard to the requirement of specific consent."[25] This has been confusing to the research community, however, given that the EU Clinical Trials Regulation states that sponsors must obtain the consent of data subjects to permit the use of their personal data collected in an interventional clinical trial for purposes outside of the primary trial protocol. Further clarity on this point would be of great assistance to the research enterprise.

Proposed Solutions

Clear guidance from the EDPB discussing instances in which industry and academic researchers can process personal data for "compatible" purposes and a reaffirmation of Recital 33's statement that consent may be broad to cover future research studies, whose specific purpose may not yet be known at the outset of the research, would reduce the current confusion in this area, and would facilitate scientific research studies.

C. *Providing Notice for Secondary Research*

GDPR requires that a controller provide the data subject a notice that contains several pieces of information regarding the processing of the data subject's data even when the controller does not collect data directly from the data subject.[26] However, the controller of personal data performing

[24]GDPR, recital 33 (emphasis added).
[25]Article 29 Working Party, Guidelines on consent under Regulation 2016/679 (rev. Apr. 10, 2018).
[26]*See* GDPR, art. 14. Note that when data are collected directly from the data subject, the notice must be provided at time of collection, *see* GDPR, art. 13, whereas when the data are collected from another source, the notice must be provided within one month of collection.

secondary research often receives only pseudonymized data and thus is not in a position to provide notice to the data subjects of any additional processing of their personal data. Apparently anticipating such a circumstance, GDPR Article 14(5)(b) allows an exception to the notice requirement when providing notice "proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical research purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. . . ."

However, there has been little guidance on the interpretation of this provision, and a recent enforcement action from the Polish Personal Data Protection Office (the "UODO") has caused concern about overly-narrow interpretations. The UODO found that a company that provided notice via email to data subjects whose email addresses it held but did not notify data subjects via traditional mail when it held only their mailing addresses had failed to identify a legally cognizable "disproportionate effort" despite the fact that the company in question maintained that mailing notices would have been cost prohibitive and might have led to termination of operations:

> *[T]he Company justifying the non-performance of an obligation arising from art. 14 paragraph 1 - 3 of Regulation 2016/679 with high financial costs, up to an attempt to transfer responsibility - if it did - for a possible decrease in its competitiveness on the market, or loss of financial liquidity, up to the need to terminate its operations, is a circumstance definitely working to the detriment of the Company. . . . Non-performance of the above obligation due to the financial costs indicated by the Company, indicates a decrease in the value of the rights of persons whose personal data the Company processes, in relation to the value of the Company's finances, which argument cannot be considered justified in the light of the requirements of Regulation 2016/679.*[27]

The UODO fined the company and ordered it to contact approximately 6 million affected data subjects, at an estimated cost of at least 8 million euros.[28] While this decision did not involve an enterprise engaged in clinical research, this decision, which is at present being challenged by the UODO, has stark implications for entities engaging in secondary research for scientific purposes. Such entities and their researchers have been alerted by this case decision that they should not and cannot rely on GDPR's Article 14 notice exception, as the holding suggests that cost, even when it would result in an entity's financial insolvency, cannot be considered "disproportionate effort." The research community would benefit from clear guidance from the EDPB discussing the instances in which providing notice would be impossible or involve disproportionate effort. In cases in which a researcher holds only pseudonymized data and does not require access to identified data to perform the research, excuse of the notice requirement would seem consistent with the principle of data minimization and in any event would more effectively protect privacy of the data subject.

Proposed Solutions

[27] *See* Decision of the President of the UODO, ZSPR.421.3.2018 (Mar. 15, 2019) https://uodo.gov.pl/decyzje/ZSPR.421.3.2018 (accessed Google Translate version of Polish-language decision).
[28] *See* IAPP Daily Dashboard, Poland's DPA issues its first GDPR fine, https://iapp.org/news/a/polands-dpa-issues-first-gdpr-fine/ (Apr. 1, 2019).

Guidance on when the exception under GDPR Article 14(5)(b) applies would be helpful to the regulated community to determine when the notice requirement may be excused for personal data processing for secondary scientific research. Guidance clarifying that the notice requirement can be excused in cases in which a researcher holds only pseudonymized data and thus lacks the contact information needed to provide notice would be particularly helpful, as this is often the case in secondary research scenarios.

Guidance could also be helpful in providing member states with a structure to exercise their authority under Recital 156, which permits them to provide "specifications and derogations with regard to the information requirements."

D. *Treatment of Certain Pseudonymized Data as Anonymized*

We have seen differing approaches across EU member states regarding whether pseudonymized data can, in some circumstances, be viewed as anonymized data in the hands of a person who lacks the means to re-identify the data. For example, we understand that the United Kingdom's Health Research Authority has stated that it will allow such an approach, at least in certain circumstances,[29] whereas the United Kingdom's Information Commissioner's Office has taken the position that pseudonymized data always remain "personal data."[30] We are aware of researchers in other countries expressing inconsistent positions as to whether pseudonymized data may ever be considered anonymized, which introduces complications for the research enterprise.

Proposed Solutions

The research enterprise would benefit from a clearer standard set by the EDPB on anonymization to facilitate data sharing. Moreover, the research enterprise would benefit from an anonymization standard under which a holder of data without the key needed to re-identify such data may be considered as holding only anonymized data, provided that appropriate measures are put in place to prevent the holder of the data from gaining access to the key or otherwise linking the data set to other data sources that may permit re-identification.

Such guidance might require that there be certain safeguards in place between the data provider and the receiving party, such as a formal data use agreement between the parties preventing the party receiving data from ever seeking or using the re-identification key. If such an interpretation were possible, it would greatly alleviate many challenges posed by GDPR for the research community, as parties receiving key-coded data would be able to regard the data as anonymized for their purposes, and they could use and transfer the data without

[29] *See* National Health Service Health Research Authority, *Controllers and personal data in health and care research*, (Apr. 19, 2018), https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/what-law-says/data-controllers-and-personal-data-health-and-care-research-context/.

[30] *See* U.K. Information Commissioner's Office, *What is personal data?*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/ ("However, pseudonymisation is effectively only a security measure. It does not change the status of the data as personal data. Recital 26 makes it clear that pseudonymised personal data remains personal data and within the scope of the GDPR.").

needing a legal basis to do so under GDPR.[31] *This could be particularly important for compliance with transparency initiatives, such as EMA Policy 0070 Phase 2, which will require publishing of individual patient data, meaning the data separately recorded for each participant in a clinical study.*[32]

E. *Role of Institutions/Sites in Relation to Research Data*

There has been a lack of clear guidance regarding whether a study site in a clinical trial is acting as a controller or as a processor in relation to the processing of research data. We understand that the United Kingdom has advocated for sites to be seen as processors, while in other EU member states, such as Italy and Germany, sites are generally seen as controllers. Under the Data Directive, the Article 29 Working Party issued guidance noting that, in a clinical drug trial, it is often the case that "both trial centres and sponsors make important determinations with regard to the way personal data relating to clinical trials are processed. Accordingly, they may be regarded as joint data controllers."[33] The role of the site affects the obligations between the site and the sponsor of the research under GDPR. For example, if the site is a joint controller with the sponsor, the parties must "in a transparent manner determine their respective responsibilities for compliance with the obligations under" GDPR.[34] Importantly, the responsibilities that must be allocated include the responsibility for responding to data subject requests and determining a mechanism through which the "essence of the arrangement shall be made available to the data subject."[35] Also, when there are joint controllers, GDPR permits the data subject to "exercise his or her rights under [GDPR] in respect of and against each of the controllers."[36] In contrast, if the site is deemed a processor of a controller sponsor, then the parties must enter into a "contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller."[37]

The differing positions of EU member states regarding when a site is a processor versus a controller creates challenges for multi-national research studies, since sponsors must enter into different types of agreements and comply with different data protection obligations for different sites in the same research study, based solely on the location of a given clinical trial site. Moreover, there does not appear to be a principled reason why study sites performing identical activities should be treated as processors in some jurisdictions and controllers in others.

---

[31]This could be achieved by updating/re-issuing the Article 29 Working Party's Opinion 4/2007 on the concept of personal data, in which example 13 contemplates that there may not be a means to identify key-coded data, making, as a legal matter, the party that lacks the key needed to link the coded data to the individual's identity not a possessor or processor of personal data.

[32]*See* European Medicines Agency, *External guidance on the implementation of the European Medicines Agency policy on the publication of clinical data for medicinal products for human use* (Oct. 15, 2018), https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/external-guidance-implementation-european-medicines-agency-policy-publication-clinical-data_en-3.pdf.

[33]*See* Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" ex. 25 (Feb. 16, 2010), https://www.pdpjournals.com/docs/88016.pdf.

[34]*See* GDPR, art. 26(1).

[35]*Id.* at art. 26(2).

[36]*Id.* at art. 26(3).

[37]GDPR, art. 28(3).

Proposed Solutions
The EDPB could issue guidance, potentially in the planned 2019 or 2020 EDPB update to the Article 29 Working Party's 2010 guidance on controllers versus processors, setting forth a uniform standard on whether study sites are viewed as joint controllers or processors vis-a-vis a study sponsor.[38] In lieu of a uniform standard, clear guidance from supervisory authorities announcing positions in individual EU member states would reduce confusion and allow sponsors of research better to anticipate the sponsor's obligations.

F. *Transfer of Personal Data Outside the EU*

As noted in the first set of case studies described above, GDPR has complicated the transfer of personal data outside of the EU, especially for secondary research. The Data Directive also contained restrictions on the cross-border transfer of personal data to countries that lack an adequacy decision, which include the vast majority of the non-EU countries, including major research centers such as Australia, China, South Africa, and the United States. Thus as a matter of pure regulation, GDPR did not change the law regarding cross-border transfers. In practice, however, since the advent of GDPR, EU-based institutions and researchers have focused more intently on issues of cross-border transfer, thus revealing challenges posed by the limitations on cross-border transfers of personal data to the research community that were not seen under the Data Directive. This appears to be for at least two reasons. First, much of the data transferred across national borders for research purposes are pseudonymized, and measures are put in place to ensure that the recipient of the pseudonymized data lacks access to the key to the code needed to re-identify the information. Under the Data Directive, many EU researchers took the position that pseudonymized data did not constitute personal data in the hands of a person who lacked the key to re-identify the data.[39] Thus under the Data Directive, such data would not have been subject to the limitations on cross-border data transfers. Second, GDPR has substantially increased the penalties for violation of data protection standards, which has caused EU institutions to be much more attentive to the law's restrictions on cross-border transfers.

Researchers have struggled to identify an appropriate condition or safeguard for cross-border transfer of personal data under GDPR. This has affected research involving the EU and third countries that lack an adequacy decision, including South Africa and the United States. For prospective research, such as interventional clinical trials, in which data subjects provide informed consent at the time they join the research project, researchers have often relied on the explicit consent of the data subject as the means to legitimize data transfer. Since the advent of GDPR, to satisfy the "explicit" consent requirement, when obtaining consent to the cross-border transfer of personal data for prospective research under Article 49(1)(a), in several countries, ethics committees ("ECs") have asked researchers to provide a detailed list of all countries that will receive data resulting from the study. However, at the outset of a research study, it is often not possible to know all of the countries to which data may be sent given the large number of collaborating parties and support service providers that are involved in multi-national research

[38] *See Article 29 Data Protection Working Party, Op. 1/2010 on the concepts of "controller" and "processor,"* WP 169 (Feb. 16, 2010), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf; *see* EDPB Work Program 2019/2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf.

[39] *See, e.g.*, United Kingdom, Information Commissioner's Office, *Anonymisation: Managing data protection risk code of practice* (Nov. 2012), https://ico.org.uk/media/1061/anonymisation-code.pdf.

studies today. In addition, when conducting secondary research, the research subjects are typically not in a position to grant consent to the transfer of their data from the EU to third countries. The parties must therefore rely on another approach for transfer of data.

Also, as noted above in the case studies, even when obtaining the consent of a data subject is possible, some regulators have taken positions that require that bases other than consent be used for certain studies. For example, German authorities have maintained that consent may not be the basis for transfer of personal data when the transplant donor was willing to consent to a transfer of personal data in connection with enrolment in a dual treatment-research study with the potential to save the life of a transplant recipient.

Although GDPR's standard contractual clauses work in some cases as an acceptable basis for transfer, these clauses present complications for research involving governmental agencies and government--owned or parastatal universities outside the EU, including the NIH. Such entities are often unable to agree to certain terms found in the standard contractual clauses, including those specifying auditing of data systems by a foreign entity and submission to the jurisdiction of foreign courts.[40] When the transferee is a governmental entity, it may otherwise enjoy sovereign immunity, a principle of international and national law that often protects sovereign governments from being summoned before courts, including the courts of another sovereign, without their consent to the proceedings.[41] Many research entities that are arms of sovereign governments either lack authorization to waive their sovereign immunity or have a policy not to waive such immunity. Moreover, the validity of the standard contractual clauses as a mechanism to permit cross-border data transfer is currently under challenge in the Court of Justice of the European Union.[42]

While GDPR provides that entities may enter into bespoke clauses that are tailored to the circumstances, such bespoke clauses must be approved by the competent supervisory authority.[43] In many EU jurisdictions, due to the lack of guidance from the EDPB on the requirements for bespoke clauses, the competent authorities have not yet established a process for the review of bespoke clauses, making this potentially helpful option unavailable to the research enterprise.[44]

In the U.S., for-profit entities have the option of self-certifying to the principles of the EU-U.S. Privacy Shield, a program administered by the U.S. Department of Commerce, to receive personal data from the EU.[45] Unfortunately, the Privacy Shield is not available to public/governmental/parastatal and not-for-profit entities because such entities do not fall within the jurisdiction of the U.S. Federal Trade Commission, which enforces the requirements of the

[40]*See* European Commission, *Standard Contractual Clauses*, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.
[41]*See, e.g.,* Jasper Finke, *Sovereign Immunity: Rule, Comity or Something Else*, 21 EUR. J. INT'L L. 853 (2010) ("A state's conduct falls within two categories: acts *iure imperii* or acts *iure gestonis*. It is either official or private. States therefore enjoy immunity as long as they act in their official capacity, but must submit to the jurisdiction of another state if they act as a private person.")).
[42]*See* Case C-311/11 (Facebook Ireland and Schrems).
[43]GDPR, Article 46(3).
[44]*See, e.g.*, United Kingdom, Information Commissioner's Office ("At present the ICO is not authorizing any such bespoke contracts, until guidance has been produced by the EDPB."), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/ (last accessed September 21, 2019).
[45]Note also that compliance of EU-U.S. Privacy Shield (*Commission Implementing Decision (EU) 2016/1250*) with EU legislation is currently being reviewed by the Court of Justice of the European Union in cases T-738/16 and C-311/18.

Privacy Shield.[46] This limitation in the Privacy Shield has been quite limiting to the research enterprise, given that much research is conducted or funded by such not-for-profit and charitable entities. In addition, it should be noted that the Privacy Shield regime is currently facing legal challenge in the Court of Justice of the European Union and thus may be invalidated, as its predecessor regime, the EU-U.S. Safe Harbor, was invalidated in 2015.[47]

As discussed in the above case studies, recently in at least one research collaboration involving the NIH, an EU research institute located in Finland agreed to permit the transfer of genetic data from Finland to the U.S. on the basis that the transfer is necessary "for important reasons of public interest."[48] Notably, this derogation to the prohibition on cross-border transfer of personal data requires that the "public interest . . . shall be recognized in Union law or in the law of the Member State to which the controller is subject."[49] GDPR's recitals provide some examples of when this provision may be relied upon, including for international data exchange between competition authorities, tax or customs administrations, financial supervisory authorities, services competent for social security matters, or for public health, such as tracing for contagious diseases and/or elimination of doping in sport.[50] EDPB's guidance on this derogation fails to provide clear guidelines as to when it can be applied, stating that ,"it is not sufficient that the data transfer is requested (for example by a third country authority) for an investigation which serves a public interest of a third country which, in an abstract sense, also exists in EU or Member State law[,]" but rather "the derogation only applies when it can also be deduced from EU law or the law of the member state to which the controller is subject, that such data transfers are possible for important public interest purposes including in the spirit of reciprocity for international cooperation."[51] Without a clearer statement of which EU or member state laws may permit transfer on this basis, EU research organizations will likely remain reluctant to permit cross-border transfers on the basis of this derogation.

Another complication that arises with using consent or "important reasons of public interest" as a condition for transfer arises under the EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (the "Guidelines"). The Guidelines suggest that Article 49 derogations may not be applied to a data transfer that occurs regularly within a stable relationship between a data exporter and a certain data importer or in instances in which the transfers are repetitive and not occasional.[52] Notably, the text of GDPR does not impose these limitations on transfers made pursuant to the Article 49 derogation that permits reliance on explicit consent of the data subject or the derogation that permits transfer on the basis of public interest.[53] Moreover, it is unclear from the Guidelines the extent to which the EDPB would consider data transfers occurring in different studies but between the same research centers as being repetitive

[46]*See* Federal Trade Commission, *Privacy Shield,* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield (last accessed September 18, 2019).
[47]*See* Cases T-738/16 (La Quadrature du Net and Others v. Commissioner) and C-311/11 (Facebook Ireland and Schrems).
[48]GDPR, Art. 49(1)(d).
[49]GDPR, Art. 49(4).
[50]GDPR, Recital 112.
[51]Article 29 Working Party, Guidelines on Article 49 of Regulation 2016/679 (Feb. 6, 2018).
[52]*See* Guidelines at § 1.
[53]By contrast, Recital 111 of GDPR provides that the derogations in Article 49 for "performance of a contract" and "establishment, exercise or defense of legal claim" may be used only when the transfer is "occasional and necessary."

or occasional, and consequently, the extent to which GDPR Article 49 may be applied in such cases.

In sum, the inability to find a suitable mechanism for transfer has led to the stalling of several research collaborations between the EU and third countries, resulting in the cessation of critical data flows as described above in the case studies.[54]

Proposed Solutions

There are some possible solutions that supervisory authorities and the EDPB could pursue, including: (1) issuance by the EDPB of guidance for the approval of bespoke clauses that would permit the competent supervisory authorities to approve bespoke clauses for specific research studies; (2) issuance of guidance stating when data processing for scientific research purposes carried out outside of the EU by a non-EU entity would fall under GDPR Article 3(2); or (3) issuance by the EDPB of guidance regarding when personal data may be transferred for research purposes on the basis of "public interest." Pursuant to GDPR Article 97, the European Commission is to submit a report on the evaluation and review of GDPR to the European Parliament and to the Council by May 25, 2020, and must address in the report the functioning of GDPR's provisions on cross-border data transfers. The Commission may request input from the Member States in preparing this report, thus presenting an opportunity for Member States to discuss the issues discussed in this paper.

G. *EU Vendors as Processors for non-EU Controllers*

GDPR's requirements for applying GDPR's restrictions on cross-border data transfers to transfers from processors established in the EU to controllers not established in the EU may dissuade controllers established outside the EU, and to which GDPR does not otherwise jurisdictionally apply, from engaging processors located within the EU. The application of this contracting requirement may lead controllers to prefer processors in other jurisdictions that do not impose similar burdens. Such a result is detrimental to EU-based processors that provide services to the research enterprise, such as central laboratories and data analytics firms.

GDPR requires that "processing by a processor . . . be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations of the rights of the controller."[55] The EDPB has made clear that when a controller not established in the EU engages a processor that is established in the EU, the controller does not become subject to GDPR by virtue of this activity; however, the processor is subject to GDPR and is required to

[54]GDPR provides that adherence to an approved Code of Conduct may also provide a mechanism for the cross-border transfer of personal data to third countries. We do not discuss the Code of Conduct mechanism in this input paper given that the EDPB's Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 do not address the use of codes of conduct as a safeguard for cross-border transfer of personal data and thus it is not clear when codes of conduct will become a viable mechanism for cross-border transfers of personal data.

[55]GDPR, art. 28(3).

abide by GDPR's requirements applicable to processors. [56] The EDPB guidance requires that the processor enter into an agreement meeting the requirements of GDPR Article 28 with the controller, but helpfully recognizes that in a case in which the controller is not itself subject to GDPR, the contract can omit language requiring that the processor "assist[] the controller . . . for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights" under GDPR, presumably because the controller in such a case would have no such obligation given the inapplicability of GDPR to its activities.

The EDPB has advised, however, that a condition or safeguard for cross-border transfer under Chapter V of GDPR is required even when only the processor is subject to GDPR. This is problematic because at present no standard contractual clauses exist for processor-controller transfers.[57] Further, obtaining consent of the data subject in such a situation is awkward, as a non-EU data subject, such as a resident of South Africa or the United States, must provide consent for his or her data to flow from the EU back to the data subject's own, less protective jurisdiction. From a policy standpoint, it is not clear why the cross-border transfer provisions of GDPR should apply in such a scenario, given that the controller's processing of personal data is not subject to GDPR and thus the data subjects are not afforded any of the rights under Chapter III of GDPR. The policy rationale behind GDPR's cross-border transfer restrictions, namely that personal data subject to GDPR should maintain the protections of GDPR wherever they are sent in the world, does not apply here because the data originate in a jurisdiction in which GDPR protections do not apply. Application of the cross-border transfer provisions thus complicates relations between non-EU controllers and EU processors while not adding meaningful protections to the affected data subjects.

Proposed Solutions

The EDPB should revise its guidance on the territorial scope of GDPR to clarify that GDPR's restrictions on cross-border transfers of personal data do not apply to transfers from a processor subject to GDPR to a controller not subject to GDPR. This will lessen concerns on the part of non-EU controllers that engaging a processor based in the EU will complicate the processing arrangement by requiring that the parties identify a condition or safeguard for cross-border transfer of personal data. Such a result would eliminate a competitive disadvantage for EU-based processors.

IV. Conclusion

While GDPR's implementation to-date has not resulted in a cohesive implementation of the regulation's many provisions that are intended to facilitate scientific research, the research community hopes that future guidance along the lines set forth in this paper will breathe new life into GDPR's research provisions. As highlighted in this paper, there are many possible solutions

[56] *See* EDPB, Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) – Version for Public Consultation (Nov. 16, 2018).
[57] *See* European Commission, *Standard contractual clauses for data transfers between EU and non-EU countries*, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (containing only clauses for EU controller to non-EU controller and EU controller to non-EU processor).

that data privacy regulators could implement under the existing legal framework to ensure respect for data subject rights while redressing some unfortunate and unforeseen impediments to research created by the existing approach to GDPR implementation.

* * *