View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Edinburgh Research Explorer

THE UNIVERSITY of EDINBURGH

Edinburgh Research Explorer

The EU General Data Protection Regulation

Citation for published version:
Dove, ES 2018, 'The EU General Data Protection Regulation: Implications for international scientific research in the digital era' Journal of Law, Medicine and Ethics, vol. 46, no. 4, pp. 1013-1030. DOI: 10.1177/1073110518822003

Digital Object Identifier (DOI):
10.1177/1073110518822003

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
Journal of Law, Medicine and Ethics

Publisher Rights Statement:
The final version of this paper has been published in
the Journal of Law, Medicine & Ethics, vol 46(4) by SAGE Publications Ltd, All rights reserved. © Edward S. Dove, 2018. It is available at:
https://journals.sagepub.com/doi/abs/10.1177/1073110518822003?journalCode=lmec

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

OPEN ACCESS

Download date: 05. Apr. 2019

The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era

Edward S. Dove*

*Edward S. Dove, PhD, is a Lecturer in Law at the School of Law, University of Edinburgh. Email: edward.dove@ed.ac.uk

Introduction

On May 25, 2018, the General Data Protection Regulation (GDPR)[1] took full legal effect across the European Union (EU) and, subsequently, the European Economic Area (EEA),[2] which together comprises 31 countries. Its impact on organizations in both Europe and around the world is immense. The GDPR is a massive (99 articles over 88 pages and 55,000 words), complex, omnibus data protection law that provides a comprehensive legal framework for the protection of Europeans' personal data, as well as for the promotion of responsible data processing for a range of legitimate purposes. It overhauls the ways in which organizations collect, use, and share personal data. It does so largely by recognizing that rapid developments in digital technology have increased the scale, scope, and speed at which personal data are collected, used, and distributed, thereby necessitating a stronger legal framework that enhances the rights of "data subjects." At first glance, one might consider the GDPR to be a Europe-centric law of little global consequence, not to mention – as some British "Brexiteers" would have it – another example of bumbling Brussels bureaucracy. On the contrary, the territorial scope of the GDPR follows the data that it protects and therefore has direct bearing on the activities of organizations based in countries around the world. It has direct impact on the conduct of biomedical research, given that much of this research relies on the use of individually-identifiable information. It is also, all things considered, a well-drafted piece of legislation that raises the standards of data protection globally.

Non-EU entities in the health research sector, such as the Secretary's Advisory Committee on Human Research Protections (SACHRP) in the United States, have raised alarm bells about the GDPR's impact on scientific research. In their words: "The application of GDPR requirements to human subjects research has alarmed many in our national research community, as the GDPR appears not [sic] have taken into account adequately the nature, process and demands of scientific and medical research."[3] In this article, I dispute such claims. I do so by describing and analyzing the implications of the GDPR for international scientific research that involves the processing of participants' personal data. Such research includes biobanking, genomic research, rare disease research, and clinical trials – all of which make increasing use of artificial intelligence, Big Data-driven cross-sectoral data mining and sharing, cloud computing, biotechnology, nanotechnology, and seamless global data flows across multiple countries.[4]

After briefly outlining the nature of data protection law in Europe and the key changes in data protection law under the GDPR, I then offer a basis on which to assess the GDPR's treatment of:

1) its territorial scope;
2) personal data;
3) conditions for processing "special categories" of personal data, including "genetic data" and "data concerning health";
4) legal bases for processing personal data, including the role of consent in the research context;

5) processing sensitive data and processing data for scientific research purposes, including derogations from data subject rights afforded under the GDPR when personal data are processed for scientific research purposes; and lastly,
6) two other important considerations, namely the ability to re-use previously collected personal data for research purposes (i.e. secondary use), and international data transfers.

This article stresses that the GDPR undeniably represents an improvement from the predecessor legislation – the 1995 EU Data Protection Directive[5] – as it provides both greater regulatory certainty *and* flexibility for scientific research. At the same time, it remains to be seen whether the new rules will be implemented across Europe in a harmonized way that delivers the clarity and certainty it promises, for researchers and research participants alike. It also remains to be seen whether the new law contributes to fostering cross-European and international trust in organizations that make use of personal data. The GDPR provides a disconcerting degree of latitude for national and EU-level specification in several areas, including scientific research. Because of the many areas where EU Member States "shall" and "may" carve out exceptions within the articles of the Regulation, Member States may pass national GDPR implementation laws (examples include the still-EU Member State United Kingdom, which has passed and implemented its Data Protection Act 2018, replacing the Data Protection Act 1998).[6] There is thus a potential for national divergence and regulatory fragmentation, undermining the very purpose of an EU Regulation, as I explain below. Further steps are needed therefore to guide researchers and support staff; improve regulatory harmonization; address a culture of caution relating to regulatory compliance; and enhance responsible data sharing for the purpose of facilitating progress in scientific research and medical discovery. This article, in addition to providing an overview of the GDPR for the uninitiated as it relates to health research, also offers a modest way through some of these sticking points.

Brief history and nature of data protection law in Europe

The European context

Data protection law has a long history in Europe and the continent's political and cultural contexts, such as secret police surveillance in East Germany, help explain a long tradition of citizens and governments alike seeking to craft a status of non-interference in individuals' private lives; indeed, the first modern data protection laws in the world were passed in the early 1970s in Germany (Hesse Data Protection Act in 1970) and Sweden (Data Act in 1973).

Unlike in countries such as the US or Canada, where the starting presumption in law is that processing personal data is lawful unless it is expressly forbidden, in Europe, processing personal data is prohibited unless there is a lawful basis that permits it. Moreover, data protection law in Europe is "omnibus," which is to say that, subject to a few exceptions such as personal data processing relating to law enforcement[7] and "purely personal or household activities,"[8] it is all-encompassing in its regulatory reach – covering private and public entities, individuals and companies, all types of data, and in all sectors. Essentially, if any data relating to a living person are being collected, used, or shared, they will be regulated. We can compare this sweeping approach to narrow, sector-specific data protection laws in the US, such as California's recently enacted California Consumer Privacy Act of 2018,[9] which applies to "businesses" (and only those which are large and for-profit), "service providers," "third parties" and "consumers," or the federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule,[10] which covers only "individually identifiable health information" (also known as "protected health information") and applies only to "covered entities and business associates."

<<Insert Box 1 around here>>

Box 1. Data protection versus privacy.

It is worth observing that in the European context, reference is made to *data protection* law (e.g. GDPR) rather than *privacy* law. Indeed, the word "privacy" is not mentioned at all in the GDPR, nor is the term "private life." Data protection and privacy are related but nevertheless distinct concepts. They should be seen as working together, especially with data protection seen as helping to ensure our freedoms and dignity, including our ability to seclude and include ourselves from and in society. Privacy, at least in its informational dimension, is a state of affairs whereby data relating to a person are in a state of non-access. It embodies a broad range of rights and values, such as the right to be let alone, intimacy, seclusion, and personhood. Data protection is a "set of legal rules that aims to protect the rights, freedoms, and interests of individuals, whose personal data are collected, stored, processed, disseminated, destroyed, etc. The definitive objective is to ensure fairness in the processing of data and, to some extent, fairness in the outcomes of such processing."[11] The aims of data protection, then, are broader than simply privacy protection, but at the same time, data protection is a crucial tool to ensure our privacy.[12]

The 1995 Data Protection Directive

European data protection law has built on the work of the OECD's non-binding Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,[13] first established in 1980, and the Council of Europe's binding 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), the latter of which has been ratified by 53 countries to date.[14] As part of the motivating desire for "ever closer Union," in the late 1980s the European Commission set out to harmonize data protection laws across the EU's Member States and encourage those Member States lacking comprehensive data protection laws (e.g. Italy, Spain, Greece) to establish them.[15] The resulting Data Protection Directive (95/46/EC), adopted in October 1995, aimed to both harmonize the protection of fundamental rights and freedoms of European citizens in respect of processing activities, and also to ensure the free flow of personal data between Member States.[16]

Under EU law, a Directive requires Member States to "transpose" the Directive into their national legislation; in other words, the national legislation must achieve the goals set by the Directive, but how they achieve these is for each national Member State to decide (see also Box 2). This has the benefit of allowing Member States to tailor the Directive to specific national characteristics – but this is also its main drawback. Permitting Member States room to maneuver in this transposition process can undermine the driving regulatory purpose behind any EU legislation: harmonization and/or approximation of laws across the Union. By the end of the first decade of the 2000s, it had become clear to many that not only was the 1995 Directive losing relevance in the age of digital technology-enabled massive, dynamic global data flows, but also that, as the GDPR states itself in the Recitals (i.e. the context-providing paragraphs that appear before the Articles), it had "not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity."[17] There were concerns that differences in the level of protection of the rights and freedoms of Europeans, in particular the right to the protection of personal data,[18] with regard to the processing of personal data in the Member States could prevent the free flow of personal data throughout the EU, constituting an obstacle to the pursuit of economic activities at the EU level, distort competition, and impede authorities in the discharge of their responsibilities under EU law.[19]

More specific to the research context, the Data Protection Directive lacked clear provisions on scientific and biomedical research; to the extent that reference to scientific research was made, it was "rather piecemeal and problematic."[20] Scientific research – and what it meant (e.g. did it cover biomedical research?) – failed to appear in a stand-alone article. By appearing in a number of places across the Directive, and written in inconsistent language without a consistent theory, scientific research often had to be worked through Member State derogation to determine "appropriate safeguards," causing regulatory disharmony, and helter-skelter implementation of internationally collaborative research.[21]

The move from Directive to Regulation

In order to ensure a consistent and high level of protection of European citizens and to remove the obstacles to flows of personal data within the EU, the European Commission, among other regulatory bodies, urged that the level of protection of the rights and freedoms of European citizens with regard to the processing of such data should be *equivalent* across all Member States, with consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms. In principle, a Regulation achieves this better than a Directive. As implied above, under EU law, a Regulation is a *binding* legislative act with no need for transposition. It is directly effective and must be applied in its entirety across the EU; as such, it does not require a national law to implement its provisions. (This said, as we will see, the GDPR also provides an unusually wide margin of maneuver for Member States to specify its rules, including for the processing of special categories of personal data, known colloquially as "sensitive data.")

Consequently, beginning in January 2012 with a European Commission draft text and culminating with its adoption in May 2016, the GDPR serves as a modern, fit-for-purpose Regulation that replaces the Data Protective Directive. The GDPR, like the Data Protection Directive, regulates the processing activities of two key actors for the benefit of "data subjects." These actors are:

- "data controllers" – persons or entities that determine the purposes and means of processing personal data, e.g. companies, researchers, universities; and
- "data processors" – persons or entities that process personal data on behalf of the data controller, e.g. cloud providers and research collaborators, in many circumstances.

The GDPR's two main objectives are to 1) safeguard the data protection rights of data subjects, who in the health research context are most likely to be research participants, and 2) promote the "free movement" of personal data within the EU.

<<Insert Box 2 around here>>

Box 2. A primer on EU law and EU data protection law terminology.

EU law

Directive: A legal act of the European Union that requires EU Member States to achieve a particular result or sets out a goal without dictating the means of achieving that result or goal, i.e. it is up to the individual countries to devise their own laws on the means to achieve the particular results or goals of the Directive. Where an EU Directive is not implemented into national law or is implemented incorrectly, the Directive can potentially be relied on directly by individuals in national courts of Member States if the relevant provision is sufficiently clear, precise and unconditional, but only in vertical cases i.e. against state/public bodies.

Regulation: A legal act of the European Union that has "direct applicability" in EU Member States simultaneously and therefore does not require Member States to implement national legislation. EU Regulations can potentially be relied on directly by individuals in national courts of Member States if the relevant provision is sufficiently clear, precise and unconditional.

Recitals: Text (often in enumerated paragraphs) that appears at the beginning of a legislative act (e.g. Directive or Regulation) that is preliminary in nature and provides an explanation of reasons for the operative provisions of the act. Recitals can be taken into account when interpreting the meaning of the act, but they are distinct from the articles of an act in that they are not legally binding.

Articles: The operative provisions of a legislative act (e.g. Directive or Regulation) that are legally binding.

Member State: The countries or territories that are party to the founding treaties of the European Union and thereby subject to the privileges and obligations of membership. Current EU Member States are: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Sweden, and the UK.

European Economic Area (EEA): An area in which the EEA Agreement provides for the free movement of persons, goods, services, and capital within the European Single Market, including the freedom to move and reside freely in any country within this area. Current members include the 28 EU member states, as well as three of the four member states of the European Free Trade Association (EFTA): Iceland, Liechtenstein, and Norway.

Third country: A country that is not an EU Member State.

EU data protection law

Data controller: The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor: A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller.

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

Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Key changes under the GDPR

Though some commentators give the impression that the GDPR represents a step-change in data protection law both in Europe and internationally,[22] this is not the case. Comparing the Data Protection Directive with the GDPR, one does sense some change – certainly at least in regards to a desire for greater precision in the law, as there is an expansion in size from the Directive's 34 articles to the Regulation's 99 articles. But the change is certainly not wholesale. The same concepts that applied in the Data Protection Directive – core principles of fair data processing,[23] core concepts of data controllers, data processors, data subjects, personal data, processing, special categories of data, strict conditions for international data transfers to so-called third countries, and so on – continue to apply in the GDPR. The GDPR also continues, disappointingly in my view, to regulate data on the basis of its form ("personal" and "special") and content, rather than its function (i.e. regulating on the basis of use and whether the processing activity is capable of identifying or individualizing a data subject).

The primary messages that will be imparted to readers, particularly to non-EU readers, in what follows is that under the GDPR, 1) continuity rather than disruption reigns and 2) to the extent international scientific research is impeded by this data protection regulation, it is no more impeded than under the Directive – and in many ways is less impeded. The GDPR instantiates in law what is already considered good scientific research practice, and obliges organizations to ensure that data processing in such a context is lawful, fair, and transparent, as well as of scientific value. This is not to deny the fact that the legislation is immense and complex, nor that the prospect of compliance is daunting.

One would be remiss not to mention changes under the GDPR that rightly can be qualified as important in the context of international scientific research, and which stand in contrast to many other countries' data protection laws. Some of these changes appear to target concerns around Big Data analytics and cloud computing. I mention several important changes:

1. **Territorial scope**. As further explained below, there is enhanced territorial scope of the GDPR: under Article 3, the law applies to establishments of controllers or processors in the EU, and to non-EU established organizations which monitor behavior of individuals in the EU or where it is apparent that such organizations intend to offer goods or services to individuals in the EU. Under the 1995 Data Protection Directive, only organizations "established" in the EU which processed personal data in the context of that establishment targeting EU data subjects were subject to European data protection laws, as were organizations if they also made use of "equipment" in the EU to process personal data.

2. **Data breach notification**. There is an enhanced obligation to report a personal data breach to data protection authorities within 72 hours of having become aware of it.[24] In contrast, under the Data Protection Directive, EU member states were free to adopt different data breach notification laws and most had no general obligation to notify or had minimal sanctions for failing to notify.

3. **Transparency and accountability**. Transparency and accountability requirements for organizations have increased. Accountability is one of the core principles relating to processing of personal data under the GDPR,[25] and data controllers must, e.g. be able to demonstrate that they have a lawful basis for each processing operation. Likewise, enhanced transparency provisions require that controllers inform data subjects, in advance of processing and in clear language, that they intend to process the subject's personal data

and identify which of the lawful bases under Article 6 allows that processing. For special category data, they must identify which exception under Article 9(2) permits processing such data. Transparency requirements also require information disclosure by controllers to data subjects regarding: the categories of personal data being processed; purposes of the processing as well as the legal basis; the name of controller and contact details (including of the Data Protection Officer, should it be required to appoint such an officer); the "legitimate interests" of the controller or third party, where applicable; the recipients or categories of recipients of the personal data, if any; the period for which the personal data will be stored; the data subject's rights under GDPR (and the extent to which they are limited under the scientific research exemption, as explained below); the right to lodge a complaint with the relevant data protection authority (e.g. the Information Commissioner's Office in the UK); the source from which the personal data originate, and if applicable, whether they came from publicly accessible sources; any automated decision-making, and, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and how appropriate or suitable safeguards are achieved in relation to any personal data transferred out of the EU.

4. **"Data protection by design."** The GDPR requires data controllers, both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical and organizational measures that apply data protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.[26] This is known as "data protection by design."

5. **Data protection impact assessments**. Where a type of data processing – in particular one using new technologies – is likely to result in a high risk to the rights and freedoms of data subjects (taking into account the nature, scope, context, and purposes of the processing), the controller must, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.[27] This is known as a "data protection impact assessment."

6. **Data Protection Officers**. Under the GDPR, there are internal record keeping requirements for organizations[28] and "Data Protection Officer" (DPO) appointment will be mandatory for controllers and processors which are public authorities or whose core activities, among other things, consist of processing on (an unfortunately undefined) "large scale" special categories of data (e.g. health-related data or genetic data).[29] Thus, a DPO will be necessary for hospitals that process patient data, and it will also likely be necessary for many universities and scientific research and medical organizations. Importantly, the DPO must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices. The individual may be a staff member or an external service provider; must provide their contact details to the relevant data protection authority; must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge; must report directly to the highest level of management; and must not carry out any other tasks that could result in a conflict of interest.

7. **Penalties**. Penalties for organizations in breach of the GDPR have substantially increased, as Facebook nearly found out in the fallout from the Cambridge Analytica scandal.[30] There is a tiered approach to penalties. Organizations can be fined up to 4 percent of annual global

turnover or €20 million (whichever is greater) for breaches of core data protection principles, data subjects' rights, or international data transfer restrictions.[31] An organization can be fined €10 million or 2 percent of annual global turnover (whichever is greater) for data security breaches, not having their records in order, not notifying the supervising authority (e.g. the data protection authority in a Member State) and data subjects about a breach, or not conducting a data protection impact assessment when obliged to do so.[32] These penalties apply to both controllers and processors, so cloud providers are not exempt from GDPR enforcement.

8. **Consent**. The conditions for consent have been strengthened to facilitate data subjects' comprehension of what they are consenting to with regard to data processing. The conditions for consent also enhance individuals' rights. For example, separate consent must be given for different purposes of processing in some situations, and consent will only be valid if it can be revoked without detriment. As explained below, consent is only one of several legal bases for data processing. Under the GDPR, a "request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language,"[33] and the "specific purpose" for the processing (including sharing) should be clearly explained (how this works, if at all, with broad consent is explained below).[34] It must be as easy to withdraw consent as it is to give it.[35] In brief, organizations must provide to data subjects a clear explanation of data processing to which they are consenting; the consent must be a genuinely, voluntarily "opt-in" act (e.g. organizations must ask people whether they would like to receive email updates, and people must then actively click a link or otherwise signal agreement); consent for additional purposes must not be bundled up with the provision of service;[36] and organizations cannot rely on silence or inactivity as "consent" (e.g. pre‑ticked boxes will not constitute valid consent).

9. **Data subject rights**. Finally, data subject rights have been enhanced in a number of areas, including:

    i. rights of data access, e.g. the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them are being processed, where and for what purpose(s); and the obligation for controllers to provide a copy of the personal data, free of charge, in an electronic format;[37]
    ii. the right of data subjects to have the data controller erase his or her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data (the so-called "right to be forgotten");[38]
    iii. the right for a data subject to receive the personal data concerning them, which they have previously provided in a "commonly used and machine-readable format," and to transmit that data to another controller (the so-called "right to data portability");[39]
    iv. the right to object to processing "on grounds relating to his or her particular situation"[40] where processing is based on Article 6(f) "legitimate interests" or Article 6(e) "task carried out in the public interest," including profiling based on those provisions; and
    v. the right for a data subject not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (i.e. a right not to be subject to

pure AI-driven decisions, or machine learning or other technologies that result in a decision about the individual such as a medical diagnosis).[41]

It bears emphasizing that a number of these enhanced data subject rights are curtailed in the scientific research context, as explained below.

<<Insert Table 1 around here>>

Table 1. Key articles in the GDPR relating to scientific research.

Article(s)	Subject matter
3	Territorial scope of the GDPR
4	Definitions (e.g. "personal data," "genetic data," and "data concerning health")
5	Principles relating to processing of personal data
6	Legal bases for processing personal data
7	Conditions for consent where consent is used as a lawful basis
9	Processing of special categories of personal data (i.e. sensitive data) and conditions under which such data may be processed – see in particular Art. 9(2)(j) (processing necessary for scientific research purposes)
13	Information to be provided where personal data are collected from the data subject
14	Information to be provided where personal data have not been obtained from the data subject
22	Data subject rights regarding automated individual decision-making, including profiling [note: this may not be derogated from under Article 89)
25	Data protection by design and by default
35	Data protection impact assessments
37-39	Data Protection Officers (DPOs)
40	Codes of conduct
44-49	Transfers of personal data to third countries or international organizations
89	Safeguards and derogations relating to processing for scientific research purposes

The long-arm territorial reach of the GDPR

The GDPR regulates the processing of EU citizens' personal data and personal data processed by entities established in the EU. This deceptively simple statement belies the fact that the GDPR has a global territorial reach, which is why entities in jurisdictions from the US to Mexico to China and in-between should be mindful of its provisions. The GDPR aims to protect personal data in the digital world, which often pays little regard to geographical boundaries. More specifically, it applies to the processing of personal data in the context of the activities of an establishment (e.g. office or site) of a controller or a processor in the EU, *regardless of whether the processing takes place in the EU or*

not.[42] The GDPR also applies to the processing of personal data of data subjects who are in the EU by a controller or processor *not* established in the EU, where the processing activities are related to:

1) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such *data subjects in the EU*; or
2) the monitoring of their behavior *as far as their behavior takes place within the EU*.[43]

In such cases, subject to a few exceptions, non-EU organizations processing the data of EU citizens will have to appoint a representative in the EU to act as their Europe-facing point of contact for individuals and local data protection authorities.[44] Finally, the GDPR applies to the processing of personal data by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law.[45]

In summary, this means that if an entity has no establishment in the EU (e.g. no facilities or staff), does not offer goods or services to data subjects in the EU, and does not monitor the behavior of data subjects in the EU, it will not be subject to the GDPR. For many US-based scientific research organizations and digital health companies, however, goods and services are routinely offered to data subjects in the EU, be it for genetic sequencing or the collection of health-related data on a smartphone app. Indeed, to the extent that consumers, customers, or participants of US-based companies temporarily reside in the EU (on holiday, work, or otherwise) *and* have data points collected through digital technology, such as wearables, mobile phones, or other personal electronic devices, the GDPR will apply. This has caused organizations such as SACHRP to complain that the GDPR's application to "incidental collection and transmission of personal data from those enrolled in research studies at US sites when they happen to be traveling in EU member states" will "hinder important [Department of Health and Human Services]-supported multi-site, trans-national research."[46] It is debatable whether the GDPR's territorial scope will be interpreted by data protection authorities so widely as to capture these incidental transmissions of personal data; at the very least, it seems an overstretch to characterize the provisions as "hindering" multi-site, trans-national research.

When are data "personal"?

The GDPR continues the EU data protection law tradition of regulating data that are considered personal. Conversely, data that are not personal are not regulated under the GDPR. Like the Data Protection Directive, the GDPR only covers data about living people from which they can be identified. According to Article 4 of the GDPR, "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.[47] The *Breyer* decision of the Court of Justice of the European Union confirms that courts take a wide interpretation of the main concepts in EU data protection law; it makes clear that "personal data" relates to an individual who is identifiable, either directly or indirectly, which means that information can be regarded as personal data even if it does not itself identify a specific person (e.g. IP addresses can constitute personal data).[48] Further indications on how to assess identifiability are given in Recital 21 of the GDPR. This Recital clarifies that the principles of data protection should apply to *any* information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of *all the means reasonably likely to be used*, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural

person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

The Data Protection Directive failed to address the significant question of whether human tissue is governed by data protection law; unfortunately, the GDPR fails to address this question as well. In *S. and Marper v. United Kingdom*,[49] the European Court of Human Rights found that DNA profiles and cellular samples could constitute personal data within the meaning of the UK's predecessor Data Protection Act 1998 as, in context of that case, they related to identified or identifiable individuals. A sound operating assumption, therefore, would be that biological material *itself* is not data governed under the GDPR (unless it has been "datafied," i.e. scanned, analyzed, sequenced, etc.), but the underlying data within biological material is governed by the GDPR, for example, DNA within a tumor sample, unless it is so incomplete that it is impossible to trace back to an individual. Under this operating assumption, biological material would need to be processed consistent with GDPR requirements, including prior to DNA sequencing and revelation of the inherent data.

Pseudonymized data

Personal data that have been pseudonymized (e.g. key-coded) still fall within the scope of personal data defined in the GDPR, depending on whether the data can identify natural persons by any means reasonably likely to be used.[50] For example, data may be pseudonymized, with identifiers separated, but if the dataset and identifiers are held by the same organization, it will still be considered personal data. This said, the converse – separating a dataset and having the identifiers held across different organizations – in itself and without additional techniques may not constitute anonymized or pseudonymized data, either.

Anonymous and anonymized data

The GDPR does not apply to anonymous data or data that have been anonymized. Anonymized data refers to data that were related to an identifiable individual when collected, but through processes of removing identifiers (e.g. through scrambling or blurring), the identity of an individual cannot be determined by a reasonably foreseeable method. Using state-of-the-art techniques, properly anonymized data prevents identification of an individual. It is worth noting that the act of anonymization itself is considered processing personal data. Unlike HIPAA, which specifies methods for de-identifying protected health information (the "safe harbor" method of de-identification and the statistical or "expert determination" method[51]), the GDPR does not specify anonymization methods.[52] This allows for greater flexibility in the legislation and for enabling data protection authorities to consider whether new methods of both anonymizing and re-identifying data mean the GDPR should apply. At the same time, researchers and organizations should be mindful of the prospect of anonymized data re-becoming identifiable data as more data are generated and linked to them. The key message to impart here is that this is not a one-off process; pseudonymization and anonymization require a watching brief to ensure that the categories are constantly monitored for falling within the law and thereby needing to comply.

When are personal data "special", i.e. sensitive?

Certain kinds of personal data are considered "special" – in other words, sensitive – under the GDPR and therefore deserving of even greater legal protection. Whereas with (regular) personal data, processing is lawful only where there is a lawful basis under Article 6, with special categories of data, processing is generally prohibited and will only be permitted if the processor meets one of 10 special

category conditions (i.e. exceptions) listed in Article 9(2). What this means is that, at least according to some interpretations, processing "special categories" of personal data requires two conditions:

1) the processing must have a lawful basis (i.e. one of the six legal bases outlined in Article 6[53]), *and*
2) it must fall within at least one of the 10 exceptions specified in Article 9(2).[54] One of these exceptions – the scientific research exception – is explained further below.

In the health context, "special category" personal data includes:

- data which reveal racial or ethnic origin;
- data concerning health (the physical or mental health of a person, including the provision of health care services);
- data concerning sex life or sexual orientation; and
- genetic data and biometric data processed to uniquely identify a natural person. Genetic data is defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Recital 35 of the GDPR makes clear that "data concerning health" includes information derived from the testing of a genetic sample, which is subtly distinct from genetic data per se. As I have written elsewhere:

> This is an unduly narrow definition, given that most genetic data does not provide "unique" information about a sole individual, but rather quite often the individual's genetic family members as well. This definition does align, however, with the law's general fixation with individual ("data subject") rather than familiar or group protections, whether for privacy violations, discrimination, or otherwise.
>
> […]
>
> It may be that those responsible for the collection and use of these data will err on the side of caution and assume that all genetic data should be treated as a category of personal data for the GDPR, even if they do not provide "unique" information about the physiology or the health of an individual (though whole genome sequence data would qualify on uniqueness grounds). If this happens, the majority of genomic research data would be covered by the legal provisions speaking to "genetic data" even when they might not be truly "unique."[55]

In the next section, I dive more deeply into several of the six legal bases under Article 6 for processing (regular) personal data – arguing in particular why consent should not necessarily be seen as the primary legal basis for processing in the scientific research context – before moving to analyze the GDPR exceptions that relate to scientific research and special categories of personal data, particularly Articles 9(2)(j) and 89.

The legal bases for processing personal data

In the human research context, consent is often the driving *modus operandi* for legitimate action and serves as a powerful ethico-legal norm; it is also often a legal requirement in research such as clinical trials. But consent to participation in research is *not* the same as consent serving as the legal basis for processing under data protection legislation. In the US, under HIPAA, "authorization" (i.e.

written signed permission) is required by an individual to allow a covered entity to use or disclose the individual's protected health information. In contrast, (informed) consent signals the individual's agreement to participate in a research study and includes a description of the study and other standard items seen in a participant information sheet/consent form. An authorization can be combined with (informed) consent to participate in research. If a covered entity obtains or receives a valid authorization for its use or disclosure of personal health information for research, it may use or disclose the information, provided it is consistent with the authorization.

In European data protection law, the concept of "authorization" does not exist. "Consent" is the standard term, but it must be stressed that consent is only one of several legal bases for processing personal data. In other words, researchers who seek to collect and use data from patients and participants may *not* need to rely on consent as their legal basis; and often in the research context, *consent is not the most appropriate legal basis*, particularly in large-scale epidemiological studies or genetic studies. This stands in contrast to SACHRP's statement that "consent is the basis most typically relied upon for processing personal data in research."[56] Undoubtedly, international guidance for scientific research is inconsistent as to when, if at all, consent is appropriate. The Declaration of Helsinki, for example, places a much higher reliance on consent for data processing in the context of research than the GDPR:

> For medical research using identifiable human material or data, such as research on material or data contained in biobanks or similar repositories, physicians must seek informed consent for its collection, storage and/or reuse. There may be exceptional situations where consent would be impossible or impracticable to obtain for such research. In such situations the research may be done only after consideration and approval of a research ethics committee.[57]

The Declaration of Helsinki and SACHRP seek to apply the same ethical norm, consent, equally to all types of human subjects research – whether body-, tissue-, or data-based – while the GDPR focus merely on data recognizes that consent may not be the optimal or most practical way of using personal data in research; other equally valid and lawful bases exist and indeed, some might be more appropriate. In other words, although researchers likely will need consent to fulfill their research ethics obligations, they should not assume this means they should *also* rely on consent to fulfill their data protection obligations, since alternative lawful bases ultimately will be much less burdensome on them, notably in terms of entailing fewer ancillary obligations. And indeed, in the international scientific research context in the GDPR era, insofar as data processing is concerned, lawful bases other than consent should be prioritized, as I explain below.

Can research based on broad consent still proceed under the GDPR?

The GDPR rules governing consent are not especially helpful for research, and there is confusion regarding the interplay of specific versus broad consent within the GDPR. This is a weakness in the legislation. The confusion is based on the language of Recital 33 and Article 6(1)(a), the latter of which covers consent to processing non-special categories of personal data, and 9(2)(a), which covers consent to processing special categories of data. Article 6(1)(a) states that personal data may be lawfully processed if "the data subject has given consent to the processing of his or her personal data for one or more specific purposes," while Article 9(2)(a) states that special categories of personal data may be lawfully processed if "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes." "Explicit consent" is also required when personal data are used in automated individual decision-making, such as profiling,[58]

and, where other exceptions are not possible,[59] in data transfers to so-called "third countries" (i.e. countries outside the EU) or international organizations.[60]

The modifier "explicit" is crucial here. As the predecessor data protection opinion body from the Data Protection Directive – the Article 29 Working Party – explained in 2016, "explicit" under the GDPR means that:

> […] the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future.
>
> […]
>
> […] in the digital or online context, a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature. In theory, the use of oral statements can also be sufficiently express to obtain valid explicit consent, however, it may be difficult to prove for the controller that all conditions for valid explicit consent were met when the statement was recorded.[61]

However, Recital 33 of the GDPR states that:

> It 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 when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

Recital 33 therefore suggests that the GDPR is amenable to broad consent in scientific research ("consent to certain areas of scientific research"), which presumably would yield to the judgement of an ethics committee ("when in keeping with recognised ethical standards for scientific research"), yet Articles 6 and 9 themselves, particularly in the latter Article's context of processing health-related and genetic data, would suggest that *only* specific consent can be lawfully used, unless the GDPR's drafters intended "certain areas [of research]" (Recital 33), "one or more specific purposes" (Article 6), and "one or more specified purposes" (Article 9) to be synonymous. This is debatable. Indeed, the Article 29 Working Party has opined that "the GDPR's "Recital 33 does not disapply the obligations with regard to the requirement of specific consent" and that a "well-described purpose" must be included in the consent to comply with the GDPR's requirements.[62] At the same time, and rather confusingly, it considers: "For the cases where purposes for data processing within a scientific research project cannot be specified at the outset, Recital 33 allows as an exception that the purpose may be described at a more general level."[63] The Article 29 Working Party's successor body, the European Data Protection Board,[64] should clarify in future guidance that it is legally acceptable under the GDPR for data subjects' consent to be obtained on a "broad basis," i.e. on a description of the "certain areas of scientific research" for which their personal data will be processed, including special categories of personal data, in the current time.

Moving beyond consent

More crucially, though, this unsettled state of affairs regarding broad consent in the GDPR speaks to why researchers should consider a legal basis other than consent for processing personal data for scientific research. As the UK's Information Governance Alliance (IGA) explains, other consent challenges also exist:

> There are challenges in ensuring that consent is valid, recorded, and that withdrawal of consent is respected. Furthermore, where consent is used as a basis, there will be a requirement to implement procedures and technical solutions to respond to the subjects' requests to rights that become engaged. For these reasons organisations should consider alternatives to consent as their basis for lawful processing and special categories condition […].[65]

Of course, researchers and organizations may continue to rely upon consent, consistent with IGA advice, if they are confident they can meet the GDPR requirements. More beneficially, though, organizations may be inclined to ask participants to consent (perhaps broadly) to participate in a research study as part of their research ethics obligations, but also inform them in the consent process that if they agree to participate, data relating to them will be processed under a *different* legal basis than consent, such as for a "task in the public interest" (explained below). This is particularly important to recognize, since if consent is used as the legal basis for processing data and a research participant withdraws consent, the controller will no longer have a legal basis to process personal data about them. For organizations that previously relied on consent for the purposes of collecting, using, or sharing data, they should verify whether the consent remains "GDPR compliant." If the existing consents do not meet the GDPR's requirements, organizations 1) must obtain "fresh" GDPR-compliant consent, or 2) ideally, identify a *different* lawful basis for data processing, and 3) ensure that the continued data processing is transparent and fair (i.e. that the data subjects rights and freedoms are not undermined through a change in processing), and if it is not, they should stop the processing.

Other legal bases: public interest and legitimate interests

So what are the relevant legal bases, other than consent, for processing personal data in the scientific research context? For processing non-special categories of personal data, as mentioned above, there are six legal bases, including consent. Under the GDPR, commercial companies and charitable research organizations will likely rely on "legitimate interests" as their legal basis for processing personal data. "Legitimate interests" has broad potential application, but these interests are overridden by the interests or fundamental rights and freedoms of data subjects that require protection of personal data, in particular where the data subject is a child.[66] As the UK's Information Commissioner's Office explains,[67] there are three elements to the legitimate interests basis. One needs to satisfy:

1) a purpose test: identify a legitimate interest (this can include commercial interests, individual interests, or broader societal benefits);
2) a necessity test: show that the processing is necessary to achieve it; and
3) a balancing test: balance it against the individual's interests, rights, and freedoms (i.e. an organization should consider whether it is using people's data in ways they would reasonably expect and which have a minimal privacy impact).

Public authorities cannot rely on the "legitimate interests" basis for any processing they do to perform their tasks as a public authority. Thus, public authorities, such as (non-private) universities

and public research institutes such as the US National Institutes of Health (NIH), when carrying out public tasks, are unable to rely on the "legitimate interests" basis. The GDPR explains the reason for this exclusion is because it is for the national legislatures to give public authorities the legal authority to process personal data;[68] i.e. public authorities should only be able to process personal data in performance of their tasks if the law has given them authorization. However, if the public authority has other legitimate purposes outside the scope of their tasks as a public authority, they can consider legitimate interests where appropriate. This will be particularly relevant for public authorities with commercial interests.

In general, public authorities instead will likely rely on a "task in the public interest or in the exercise of official authority vested in the controller" as their legal basis.[69] It should be noted that the interpretation of "public task" is narrow and such public tasks must be laid down by law through statutory, common law, or other legal power.[70] Public authorities should document their justification for reliance on this basis, by reference to their public research purpose as established by statute or charter. This assures participants and the public that the organization is credible and using personal data for the public good. While there is no difference in regulatory standards between organizations that use "legitimate interests" and those that use a "task in the public interest" as legal bases, the GDPR requires organizations to be explicit about which of the legal bases they are using.

Processing sensitive data and processing data for scientific research purposes

The final text of the GDPR should be a cause for celebration by the scientific research community.[71] Previous versions, particularly the one emanating from the European Parliament in 2014, alarmed the community due to their disproportionate, heavy-handed approach to regulating research. Scientific research is defined broadly in the final text of the GDPR and should be interpreted to encompass medical and biomedical research, terms that do not appear explicitly in the GDPR:

> For the purposes of this Regulation, the processing of personal data for scientific research purposes *should be interpreted in a broad manner* including for example technological development and demonstration, fundamental research, applied research and privately funded research. […] Scientific research purposes should also include studies conducted in the public interest in the area of public health.[72]

As already mentioned, the GDPR grants some exemptions from its requirements when personal data are processed for scientific research. Article 9(2)(j) permits special categories of personal data to be processed for scientific research purposes, in accordance with Article 89 based on EU or Member State law that must be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject. As the UK's Health Research Authority notes, Article 9(2)(j) and Article 89 mean that researchers can, for example, keep patient health data for very long term, refuse to delete personal data if the data subject withdraws their consent for the research, and use data from one research project for others.[73] However, as mentioned above, these exemptions apply only if appropriate safeguards are in place, for example adhering to the principle of data minimization and aiming to first anonymize, and if not possible, then pseudonymize all data where possible. Such processing must also have a basis in EU or Member State law.

I now proceed to explore Article 9(2)(j) and Article 89 in further detail.

The scientific research exception to process sensitive data

As mentioned above, one common interpretation of the GDPR is that processing special (i.e. sensitive) categories of data such as health-related data and genetic data is prohibited unless one has both a lawful basis for processing (under Article 6) *and* a special category condition (i.e. exceptions to the general prohibition) for processing in compliance with Article 9.

In the health context, exceptions exist where processing is necessary for medical diagnosis, the provision of health or social care (note that it does not expressly include medical research), treatment or management of health or social care systems in accordance with EU or Member State law or professional obligations,[74] and where data processing is necessary for public health and in the public interest on the basis of EU or Member State law.[75]

When processing special categories of data for scientific research purposes, the most likely relevant exception will be Article 9(2)(j): that such processing is necessary for scientific research in accordance with Article 89(1) and that appropriate safeguards are provided for.[76] The processing must also be consistent with EU or Member State law (such as laws relating to clinical trials). Though "appropriate safeguards" are not spelled out in the GDPR, as an exhaustive list of safeguards would be contrary to the risk-based approach that underpins the Regulation, in the scientific research context they would likely include: 1) ensuring that the research will not cause substantial damage or distress to the data subject; 2) ensuring that the scientific research project has approval from a competent and independent research ethics committee; and 3) ensuring that the data controller has technical and organizational safeguards in place that ensure respect for the principle of data minimization and ensure that exemptions to data subjects' rights are not exercised unless the rights are likely to render impossible or seriously impair the achievement of the purposes of the processing. Examples would include pseudonymizing personal data where compatible with the research purpose, and avoiding processing identifiable data where the research purpose can be fulfilled by further processing with anonymized data. Other examples include having robust IT security and data protection policies in place, as well as risk-assessment exercises of data systems, regular review and audit of privacy impact assessments, and developing efficient IT systems, policies, and procedures to handle data subjects' requests.

Organizations must include the legal basis for processing data in a privacy notice made available to data subjects (sometimes also known as a "fair processing notice"), which includes contact details for the Data Protection Officer, the purposes and legal basis for processing data, and information about with whom data are shared. Best practice suggests that this should be provided at a general level in organizational documents, and project-specific details should be provided to participants in documents such as newsletters or participant information sheets (i.e. consent forms). This information should be given to data subjects prior to processing their personal data, or, where the personal data are obtained from another source (i.e. from another organization), within a reasonable period, depending on the circumstances of the case.[77] The GDPR helpfully clarifies that where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.[78]

Safeguards and derogations related to processing data for scientific research purposes

Article 89(1) states that processing personal data for scientific research purposes (as well as archiving purposes in the public interest and historical research purposes) must be subject to "appropriate safeguards […] for the rights and freedoms of the data subject." These safeguards are meant to ensure that technical and organizational measures are in place, in particular, to ensure the

principle of data minimization (limiting personal data collection, storage, and usage to data that are relevant, adequate, and absolutely necessary for carrying out the purpose for which the data are processed). This means that anonymization or pseudonymization should be used wherever possible.

Crucially, Article 89(2) allows member countries to create derogations from (i.e. exceptions to) the otherwise core data subject rights of data access, to rectification, to erasure, to be forgotten, to restriction of processing, and to object,[79] whenever these data subject rights "are likely to render impossible or seriously impair the achievement" of scientific research purposes. Such a derogation must be essential for the fulfillment of these purposes. These derogations are subject to the conditions and safeguards laid out in Article 89(1), such as data minimization and pseudonymization (Recital 156).

The "right to object" is curtailed in a slightly different manner than the other data subject rights. Article 21(6) gives data subjects an unconditional right to object in the context of scientific research, as opposed to the conditional right to object in general contexts afforded by Article 21(1). By "unconditional," I mean that the data controller cannot refuse the request by demonstrating a compelling legitimate ground. Yet, even in the scientific research context, this right is still subject to certain restrictions, namely it can be overridden where "the processing is necessary for the performance of a task carried out for reasons of public interest."[80] Article 89(2), on the other hand, serves a slightly different purpose. It allows Member States and the EU to lay down further restrictions on such an "unconditional" right to object, in addition to the "public interest" exception, so long as the Member State (or EU) can show that two conditions are fulfilled: (1) the exercise of this right is "likely to render impossible or seriously impair the achievement of the specific purposes"; and (2) the restrictions are "necessary for the fulfilment of those purposes." In short, this means that in the absence of national legislation, data controllers may invoke Article 21(6) to refuse the data subject's right to object on the ground that the processing is necessary for the performance of a task carried out for reasons of public interest. Where national laws are in place, and they are in line with the conditions set out in Article 89(2), data controllers may invoke such laws to process personal data for non-public interests. Thus, Article 89(2) allows for expansion of the exception set out by Article 21(6), by means of Member State and EU legislation.

Other important GDPR considerations for international scientific research

There are two other important issues to consider in assessing the GDPR's impact on international scientific research: secondary data use and international data transfers.

Secondary data use

An increasing amount of scientific research relies on access to and use of data collected from previous studies or other contexts. The GDPR has a favorable provision for secondary data use in the research context. Ordinarily, a strict "purpose limitation" principle applies: personal data must not be further processed in a manner that is incompatible with the specific and legitimate purposes for which they were originally collected and processed.[81] However, Article 5(1)(b) states that further processing for scientific research purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial data processing purposes. This means that if the same or another organization were conducting the further processing (i.e. secondary use) of the data, there is a rebuttable presumption that further processing for the purpose of scientific research is compatible with the original stated purpose of the processing (which might be for e.g. medical diagnosis). The derogations from data subject rights that the scientific research exception permits under Article 89(2) would apply in such a scenario, as permitted by applicable Member State law.

International data transfers

International scientific research collaboration is affected by the GDPR rules on transferring personal data from the EU to a non-EU country, known as a "third country." Data controllers that plan to transfer Europeans' personal data to a third country or international organization, be it for cloud computing purposes or otherwise, must be mindful of the GDPR's provisions on international data transfers. There are four avenues for lawful transfer of personal data outside the EU:

1) an adequacy decision (Art. 45);
2) appropriate safeguards (Arts. 46 and 47);
3) specific derogations (Art. 49); and
4) exceptions for one-off (or infrequent) transfers (second subparagraph of Art. 49(1)).

A controller must inform data subjects, at the time that personal data are collected from them, that the controller intends to transfer this personal data to a third country or to an international organization, and that either a) an adequacy decision either exists or is absent, or b) in the case of transfers referred to in Article 46 or 47, or one-off (or infrequent) transfers, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Data can be transferred to a country outside of the EU or to an international organization without specific authorization, provided the country or region's relevant legal framework has been assessed by the European Commission as having an "adequate level of protection" (referred to as an adequacy decision).[82] To date, the Commission has recognized as adequate the countries or territories of Andorra, Argentina, Canada (limited only to commercial organizations subject to the federal Personal Information Protection and Electronic Documents Act), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, and the US (importantly limited to the Privacy Shield framework[83]). Adequacy talks are ongoing with South Korea. Only US legal entities subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DOT) are eligible to participate in Privacy Shield; thus, it is unlikely that US universities and publicly funded research sponsors, among other entities, can rely on the framework for non-commercial purposes.[84]

In the absence of an adequacy decision, data can still be transferred to a third country or to an international organization if the data controller or processor has appropriate safeguards and enforceable data subject rights, and effective legal remedies are available. Adequate safeguards may be provided for by:[85]

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organizations within a corporate group) if approved by the competent supervisory authority;
- standard data protection clauses in the form of template transfer clauses adopted by the European Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a data protection authority and approved by the European Commission;
- compliance with an approved code of conduct pursuant to Article 40 that has binding and enforceable commitments (see discussion in Conclusion below for a code of conduct being drafted in the health research space);
- certification under an approved certification mechanism as provided for in the GDPR that has binding and enforceable commitments;

- contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization, which are authorized by the competent data protection authority; or
- provisions inserted into administrative arrangements between public authorities or bodies authorized by the competent data protection authority.

Standard data protection clauses or contractual clauses may not be a viable option for some non-EU public authorities or organizations out of concerns regarding compliance with, among other things, indemnification and jurisdiction clauses.

A third avenue for lawful transfer of personal data outside the EU is derogations for specific situations. Obtaining explicit consent from the data subject "to the proposed [international] transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards"[86] is one derogation option. However, this rubs against the general desire to avoid relying on (explicit) consent as the legal basis for processing personal data for scientific research purposes, for the reasons explained above. This option is also not available for the activities of public authorities in the exercise of their public powers.[87] Another potentially relevant derogation option is a transfer, or set of transfers, "necessary for important reasons of public interest."[88] Yet again, the GDPR enables Member States to determine individually "where important grounds of public interest laid down" require international transfer.[89] It is unclear if international scientific research would fall under this derogation option; the GDPR Recitals mention only cases of "public health, for example in the case of contact tracing for contagious diseases."[90] For this reason, it is expected that research organizations may have to rely on the fourth avenue for lawful international data transfer.

The fourth avenue for a lawful international data transfer is where a transfer could not be based on a provision in Article 45 (adequacy decision) or Article 46 (appropriate safeguards), and none of the derogations for a specific situation referred to in Article 49 is applicable (e.g. explicit consent or important reasons of public interest). In such a "residual case" scenario,[91] a transfer to a third country or an international organization may take place only if the transfer:

- is not being made by a public authority in the exercise of its public powers;
- is not repetitive (i.e. similar transfers are not made on a regular basis);
- involves data related to only a limited number of individuals;
- is necessary for the purposes of the compelling legitimate interests of the organization (provided such interests are not overridden by the interests of the individual); and
- is made subject to suitable safeguards put in place by the organization (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data.

The GDPR specifically mentions that: "For scientific […] research purposes […], the legitimate expectations of society for an increase of knowledge should be taken into consideration"[92] in permitting transfers in this scenario. Examples might include a rare disease organization based in Heidelberg that wants to share a dataset containing personal and pseudonomyzed data of four patients to an academic medical center in Chicago for genotype-phenotype matching. In cases falling under this "residual cases" avenue, organizations are obliged to inform the relevant data protection authority of the transfer and provide additional information to individuals on the international data transfer.

Given all four of these avenues are not ideal for smooth international data transfers, it is all the more reason, as further discussed below, to have a code of conduct for scientific (health) research in

place as soon as possible to enable international data transfers of health-related and genetic data on a legal basis other than explicit consent.

Finally, it should be mentioned that as anonymized data are not subject to GDPR requirements, such data can transferred outside of the EU without being subject to any of the above requirements. Pseudonymized data could in some cases be considered not to be personal data, though this remains contested; a safer assumption is that such data are personal and thus are subject to these international transfer requirements.

Conclusion

Overall, the GDPR should be welcomed as an advancement in data protection law that enables scientific research to flourish in a responsible manner. The Regulation represents neither a step-change in either data protection law, nor in how scientific research, local and international, is conducted. Moreover, ethics committees will continue to undertake their review of research projects in much the same way; ethico-legal norms of consent, privacy, and confidentiality will endure. What the GDPR does do is raise the standards globally for best practices in data protection. It also commands researchers and others to consider the importance of respecting individuals' data, and the legal bases on which they rely to collect and use that data for research. More often than not, the GDPR will *not* necessitate wide-scale changes in current practice, including the much-dreaded fear of re-consenting research participants. Rather, the GDPR obligates researchers and organizations to beef up their policies on accountability, transparency, safeguards, data subjects' rights, and research exemptions. Thus, I disagree with the sentiment expressed by organizations such as SACHRP that because the GDPR diverges from narrow, sector-specific legislation such as HIPAA, it is per se problematic. On the contrary, though far from perfect (as we see, for example, in the confusion regarding specific and broad consent and in the strict provisions on international data transfers), the GDPR should encourage countries such as the US to raise their standards of data protection and achieve regulatory harmonization with the EU. Few would consider the reverse scenario beneficial to participants and publics.

While this article stresses that the GDPR does not represent a step-change in data protection law, and should not be interpreted as an onerous, draconian regulation for research, nevertheless there are crucial steps that non-EU research organizations should take if they find themselves collecting or otherwise using Europeans' personal data. Included among these steps are:[93]

- discussing the implications of the GDPR with researchers and research managers and potentially appointing a Data Protection Officer;
- establishing what data their organization is controller for and which data researchers are processing on behalf of another organization;
- knowing what kinds of personal data and special categories of personal data researchers are currently processing;
- determining how their organization will comply with the organization and technical safeguards for the scientific research exemption;
- determining how best to apply the research exemptions to data subject rights;
- ensuring that their organization complies with the transparency requirements of the new legislation; and
- determining whether research participants were ever previously informed about the legal basis on which they are processing data about them (and if so, verifying whether it is a correct legal basis under the GDPR; and if not, informing them of the legal basis in a privacy notice); and

- determining whether any personal data will be internationally transferred outside the EU, and if so, the lawful grounds on which such transfer can occur.

If there is an overarching concern to highlight, it is that the GDPR risks becoming as much a Directive as a Regulation, particularly in the scientific research context. We see that just as with the Data Protection Directive, a significant amount of room is permitted for Member States to determine national appropriate safeguards for processing data for scientific research purposes.[94] For example, Member States can provide in their national legislation that health-related and genetic data may not be processed at all, or impose additional conditions for processing such data. Each Member State can also choose which of the five following individual data subject rights will be limited in their national law: to access data; to rectify inaccurate data; to restrict processing; to object to processing; and whether the right of a child to have the erasure of personal data concerning him or her without undue delay, i.e. the "right to be forgotten" (if necessary for the processing), can be restricted for research purposes. Member States may also provide for additional safeguards and set out conditions and safeguards for any national derogations or exemptions granted for scientific research purposes. Further steps are needed therefore to guide researchers and support staff;[95] improve regulatory harmonization; reduce a culture of caution relating to regulatory compliance; and enhance responsible data sharing for the purpose of facilitating progress in research and medical discovery.

Towards this end, the Biobanking and BioMolecular resources Research Infrastructure-European Research Infrastructure Consortium (BBMRI-ERIC),[96] a European-based distributed research infrastructure of biobanks and biomolecular resources that provides expertise and services on a non-economic basis and facilitates access to collections of partner biobanks and biomolecular resources, is currently developing a "Code of Conduct for Health Research," in line with GDPR Article 40.[97] This works around the GDPR's drawback of permitting EU Member States to derogate from a number of data subjects' rights when health, biometric, or genetic data are used for scientific research purposes. Article 40 encourages associations and other bodies representing categories of controllers or processors to draw up codes of conduct as a way to help them apply the GDPR effectively and allow them to demonstrate their compliance. It is an example of sound co-regulation, where the content and enforcement mechanisms remain under control of the data protection authorities and overall approval is subject to European Data Protection Board and European Commission approval. A Code of Conduct for Health Research will help ensure there is authoritative health research sector-specific guidance on implementing the GDPR that can apply not only across the Member States, but internationally. More crucially, public and private organizations could rely on the Code of Conduct rather than specific Member State derogations to share personal data across borders, including from the EU to countries such as the US and Canada. Indeed, the GDPR permits an EU organization to transfer personal data to a third country or an international organization through an approved code of conduct, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.[98] Ideally, then, this Code of Conduct for Health Research will help stymie the difficulties for cross-border research that could arise as Member States implement domestic legislation with different derogations for research. Ultimately, even beyond the development of a Code of Conduct for Health Research, greater international coordination is needed to seek legal interoperability across countries and regions, both within and outside Europe.[99] The basis for that coordination, though, should be the GDPR rather than other data protection laws that provide weaker rights for citizens.

Acknowledgements

Special thanks to Graeme Laurie, Mark Taylor, Mark Rothstein, Niamh Nic Shuibhne, Annie Sorbie, Jiahong Chen, and Mark Phillips for their insightful comments on an earlier draft. A very condensed version of this article appeared as a "GDPR Primer" distributed via electronic communication by the Global Alliance for Genomics and Health (GA4GH) in September 2018 and was co-authored by the GA4GH's GDPR and International Health Data Sharing Forum, of which this author is chair and lead editor: https://www.ga4gh.org/.

References

1. 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) [hereinafter GDPR].
2. Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]. Membership of the EEA has grown to 31 states as of 2018: the 28 EU member states (which still includes the United Kingdom as of the time of writing), as well as three of the four member states of the European Free Trade Association (EFTA): Iceland, Liechtenstein, and Norway. The other EFTA member, Switzerland, has not joined the EEA, but has a series of bilateral agreements with the EU that allows it also to participate in the internal market. Switzerland is currently revising its Federal Act on Data Protection to accord with the GDPR and maintain its "adequacy" status under Art. 45 of the GDPR.
3. Secretary's Advisory Committee on Human Research Protections (SACHRP), "Attachment B - European Union's General Data Protection Regulations," March 13, 2018, *available at* <https://www.hhs.gov/ohrp/sachrp-committee/recommendations/attachment-b-implementation-of-the-european-unions-general-data-protection-regulation-and-its-impact-on-human-subjects-research/index.html>.
4. Dove, E.S., Phillips, M., "Privacy Law, Data Sharing Policies, and Medical Data: A Comparative Perspective," in Gkoulalas-Divanis, A., and Loukides, G., eds., Medical Data Privacy Handbook (Cham: Springer, 2015). See also Information Commissioner's Office (ICO), Big Data, Artificial Intelligence, Machine Learning and Data Protection (2017), *available at* <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>; House of Lords Select Committee on Artificial Intelligence, AI in the UK: Ready, Willing and Able? (2018), *available at* <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>.
5. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [hereinafter Data Protection Directive].
6. In theory, the GDPR has direct effect in Member States and its default rules are always in place in the absence of national legislation. For an up-to-date list of EU Member State GDPR implementation laws and drafts, see IAPP, "EU Member State GDPR Implementation Laws and Drafts," *available at* <https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/>. See also Fazlioglu, M., "What the GDPR Requires of and Leaves to the Member States," *available at* <https://iapp.org/media/pdf/resource_center/GDPR-Derogations-Whitepaper-FINAL.pdf>.
7. Under Article 2(d) of the GDPR, processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the

execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, is subject not to the GDPR, but rather to a separate EU law: Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (otherwise known in shorthand as the Law Enforcement Directive).

8. GDPR, Art. 2(c).
9. California Consumer Privacy Act of 2018, A.B. 375. See generally de la Torre, L., "GDPR matchup: The California Consumer Privacy Act 2018," IAPP Privacy Tracker, July 31, 2018, *available at* <https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/>.
10. HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information: Final Rule"), 45 CFR Part 160 and Subparts A and E of Part 164.
11. Tzanou, M., "Data Protection as a Fundamental Right Next to Privacy?" International Data Privacy Law 3, no. 2 (2013): 88-99, at 89.
12. Poullet, Y., "Is the General Data Protection Regulation the Solution?" Computer Law & Security Review 34, no. 4 (2018): 773-778, at 778.
13. OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, revised 2013), *available at* <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.
14. Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108 (1981), *available at* <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. In 2018, the Council of Europe adopted an amending Protocol which updates Convention 108. As with Convention 108, the amending Protocol is open to any country in the world to sign. *See* Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (2018), *available at* <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf>.
15. For a more complete history, see Bygrave, L. A., Data Privacy Law: An International Perspective (Oxford: Oxford University Press, 2014), at 54-56.
16. Data Protection Directive, *supra* note 5, Recitals 3, 5, 7 (promoting data flow across the EU) and Recitals 2, 3, 10, 11 (emphasizing the importance of protecting data subjects' rights).
17. GDPR, Recital 9.
18. Charter of Fundamental Rights of the European Union (2000/C 364/01), Art. 8(1) ("Everyone has the right to the protection of personal data concerning him or her.")
19. GDPR, Recital 9. See also Poullet, Y., "EU Data Protection Policy. The Directive 95/46/EC: Ten Years After," Computer Law & Security Review 22, no. 3 (2006): 206-217, at 206.
20. Townend, D., The Politeness of Data Protection: Exploring a Legal Instrument to Regulate Medical Research Using Genetic Information and Biobanking (PhD thesis, Maastricht University, 2012), at 48.
21. *Id*. See also D. Beyleveld et al., eds., Implementation of the Data Protection Directive in Relation to Medical Research in Europe (Aldershot: Ashgate, 2004).
22. See e.g. Albrecht, J.P., "How the GDPR Will Change the World," European Data Protection Law Review 2, no. 3 (2016): 287-289.
23. GDPR, Art. 5.
24. GDPR, Art. 30(1).
25. GDPR, Art. 5.
26. GDPR, Art. 25.
27. GDPR, Art. 35.

28. GDPR, Art. 30.
29. GDPR, Art. 37. The UK's Information Commissioner's Office (ICO) somewhat explores the meaning of "large scale" and points out a DPO will be necessary for hospitals that process patient data. See Information Commissioners' Office, "Consultation: GDPR DPIA Guidance" (2018), *available at* <https://ico.org.uk/media/about-the-ico/consultations/2258459/dpia-guidance-v08-post-comms-review-20180208.pdf>.
30. In July 2018, due to the timing of the breaches, Facebook was fined £500,000 by the UK's Information Commissioner's Office, which was the highest allowed under the predecessor Data Protection Act 1998. See Hern, A., Pegg, D., "Facebook Fined for Data Breaches in Cambridge Analytica Scandal" The Guardian, July 11, 2018, *available at* <https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal>.
31. GDPR, Art. 83(5).
32. GDPR, Art. 83(4).
33. GDPR, Art. 7(2).
34. GDPR, Art. 6(1)(a).
35. GDPR, Art. 7(3).
36. GDPR, Art. 7(4).
37. GDPR, Art. 15.
38. GDPR, Art. 17.
39. GDPR, Art. 20.
40. GDPR, Art. 21.
41. GDPR, Art. 22.
42. GDPR, Art. 3(1).
43. GDPR, Art. 3(2).
44. GDPR, Art. 27. Importantly, this obligation does not apply to data processing which is 1) occasional, 2) does not include, on a large scale, processing of special categories of data (e.g. health-related data and genetic data), and 3) is unlikely to result in a risk to the rights and freedoms of data subjects, taking into account the nature, context, scope, and purposes of the processing. The obligation also does not apply to data processing performed by a public authority or body.
45. GDPR, Art. 3(3).
46. SACHRP, *supra* note 3.
47. GDPR, Art. 4(1).
48. *Patrick Breyer v. Bundesrepublik Deutschland*, Case C‑582/14 (October 19, 2016). This case involved the predecessor 1995 Data Protection Directive, but the *ratio* endures.
49. *S. and Marper v. United Kingdom* [2008] ECHR 1581, Application nos. 30562/04 and 30566/04.
50. See M. Mourby et al., "Are 'Pseudonymised' Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK," Computer Law & Security Review 34, no. 2 (2018): 222-233. Mourby and colleagues argue convincingly that pseudonymized data can produce anonymous data for third parties, provided that pseudonymization is irreversible and re-identification is impossible as far as third parties are concerned.
51. 45 CFR § 164.514(b).
52. In 2014, the Article 29 Data Protection Working Party issued an Opinion that highlighted various anonymization techniques and assessed their merits. This Opinion still has resonance under the GDPR. See Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (WP216) (2014).
53. These six legal bases are: (1) consent from the data subject; (2) necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (3) necessary for compliance with a legal obligation to which the controller is subject; (4) necessary in order to protect the vital interests of the data

subject or of another natural person; (5) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and (6) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

54. GDPR, Art. 9(2)(a)-(j). Some Member States based in the civil law tradition (e.g. Germany), however, adopt the Roman law principle that when there is a general condition and a specific condition, the specific condition replaces the general. Thus, in this case, they take the position that Article 9 is *lex specialis*, i.e. a specific (special) condition about the legal basis for processing that replaces the general Article 6 requirements. They see this as important in preventing the circumvention of the high barriers introduced by Article 9 – especially compared to Art. 6(1)(b) and Art. 6(1)(f) – which has no equivalent in Article 9. Other Member States, including those based on common law tradition (i.e. the UK) do not take this position and adopt the one mentioned in the main text of this article. See generally, Molnár-Gábor, F., "Germany: A Fair Balance between Scientific Freedom and Data Subjects' Rights?" Human Genetics (forthcoming).
55. Dove, E.S., "Collection and Protection of Genomic Data," in S. Gibbon et al., Routledge Handbook of Genomics, Health and Society (New York: Routledge, 2018), at 163-64.
56. SACHRP, *supra* note 3.
57. Declaration of Helsinki (2013), para. 32.
58. GDPR, Art. 22(2)(c). An exception to this obligation is either where the automated decision is necessary for entering into, or performance of, a contract between the data subject and a data controller; or is authorized by EU or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.
59. These exceptions to the general rule prohibiting transfer of Europeans' personal data to third countries are an adequacy decision pursuant to GDPR, Art. 45(3) and "appropriate safeguards" pursuant to Art. 46.
60. GDPR, Art. 49(1)(a).
61. Article 29 Working Party, Guidelines on consent under Regulation 2016/679 (WP259 rev.01) (2016), at 18-19.
62. *Id*., at 28.
63. *Id*.
64. The European Data Protection Board has replaced the Article 29 Working Party as the independent European body that contributes to the consistent application of data protection rules throughout the European Union, and that promotes cooperation between the EU's data protection authorities. See European Data Protection Board, *available at* <https://edpb.europa.eu/edpb_en>.
65. Information Governance Alliance, "The General Data Protection Regulation: What's New," *available at* <https://digital.nhs.uk/binaries/content/assets/legacy/pdf/1/n/iga_-_gdpr_what%27s_new_guidance_v1_final.pdf>, at 15. The core members of the Information Governance Alliance are the Department of Health, NHS England, NHS Digital, and Public Health England.
66. GDPR, Art. 6(1)(f). See also M.J. Taylor et al., "When can the Child Speak for Herself? The Limits of Parental Consent in Data Protection Law for Health Research," Medical Law Review 26, no. 3 (2018): 369-391.
67. Information Commissioner's Office, "Guide to the General Data Protection Regulation: Legitimate Interests," *available at* <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>.
68. GDPR, Recital 47.

69. GDPR, Art. 6(1)(e). The Explanatory Notes to the UK's Data Protection Act 2018, example, state that "a [public] university undertaking processing of personal data necessary for medical research purposes in the public interest should be able to rely on [GDPR] Article 6(1)(e) [i.e. performance of a task carried out in the public interest]." See Explanatory Notes, Data Protection Act 2018, at para. 85, *available at* <http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf>.
70. GDPR, Recital 41 and Art. 6(3).
71. For previous discussion of a draft version of the GDPR as well as the final version, and its implications for scientific research, see Dove, E.S., Townend, D., Knoppers, B.M., "Data Protection and Consent to Biomedical Research: A Step Forward?" Lancet 384, no. 9946 (2014): 855; Dove, E.S., Thompson, B., Knoppers, B.M., "A Step Forward for Data Protection and Biomedical Research," Lancet 387, no. 10026 (2016): 1374-1375.
72. GDPR, Recital 159 (emphasis added).
73. Health Research Authority, "Safeguards," *available at* <https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/safeguards/>.
74. GDPR, Art. 9(2)(h).
75. GDPR, Art. 9(2)(i).
76. GDPR, Art. 9(2)(j).
77. GDPR, Recital 61. See also Health Research Authority, "GDPR Guidance," *available at* <https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/>.
78. *Id*.
79. GDPR, Arts. 15, 16, 18, 21.
80. GDPR, Art. 21(6).
81. GDPR, Recital 50 and Art. 5(1)(b).
82. GDPR, Art. 45(1). See also Stoddart, J., Chan, B., Joly, Y., "The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research," Journal of Law, Medicine & Ethics 44, no. 1 (2016): 143-155.
83. Privacy Shield Framework, *available at* <https://www.privacyshield.gov/welcome>.
84. Privacy Shield Framework, "FAQs," *available at* <https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1>.
85. GDPR, Arts. 46(2) and (3), 47.
86. GDPR, Art. 49(1)(a).
87. GDPR, Art. 49(3).
88. GDPR, Art. 49(1)(d).
89. GDPR, Recital 111.
90. GDPR, Recital 112.
91. GDPR, Recital 113.
92. *Id*.
93. See also Health Research Authority, "GDPR Guidance," *supra* note 77.
94. See GDPR Arts. 6, 8, 9, 22, 89. In the non-scientific research context, Member State derogations are also allowed in GDPR Arts. 10, 23, 36, 37, 38, 49, 58, 83, 87, 88, and 90. See generally Fazlioglu, *supra* note 6.
95. For a theoretically-based argument as to why guidance is important, see G. Laurie et al., "Charting Regulatory Stewardship in Health Research: Making the Invisible Visible?" Cambridge Quarterly of Healthcare Ethics 27, no. 2 (2018): 333-347.
96. See BBMRI-ERIC, *available at* <http://www.bbmri-eric.eu/>.
97. See Code of Conduct for Health Research, *available at* <http://code-of-conduct-for-health-research.eu/>.
98. GDPR, Art. 46(2)(e).

99. On this point, see also Dove, E.S., “Biobanks, Data Sharing, and the Drive for a Global Privacy Governance Framework,” Journal of Law, Medicine & Ethics 43, no. 4 (2015): 675-689.