Comments on ***Guidelines 2/2020 on articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies***

This letter is from the International Society for Biological & Environmental Repositories (ISBER) in response to a request for comments on the ***Guidelines 2/2020 on articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies.***

Introduction:

The International Society for Biological and Environmental Repositories (ISBER; www.isber.org) is a global organization of experts in biobanking and biospecimen research with knowledge and experience in GDPR's implications for biospecimens and associated data sharing globally. ISBER membership and thought leaders are recognized for their extensive knowledge and experience in the area of human biospecimens and associated data used for global research. Their expertise is extensive, longstanding, ongoing and representative of best practices followed worldwide.

Biorepositories and biobanks involve the collection, processing, storage, and distribution of human biospecimens and data for research. Research on biospecimens and associated personal health care data has led to major advancements in medical care. For example, research on residual biospecimens and associated data have led to targeted treatments for many cancers and other diseases. Such research advances often require large numbers of biospecimens and associated personal health and clinical data obtained from multiple biobanks. In many cases, such research may only be conducted by extensive biospecimen and data sharing through international research collaborations between researchers and biobanks in the EU and those external to the EU.

The GDPR has important implications for these exchanges of biospecimens, associated personal data and the research such exchanges are intended to support. A number of challenges have been encountered in these collaborations, particularly for secondary research involving biospecimens and associated data, where it is not possible to obtain a new consent and for the transfer of specimens with associated personal data outside the EEA for important research, particularly between public entities.

As such, ISBER has a keen interest in the GDPR and its implications for research, particularly with regard to the GDPR's territorial reach and transfers of personal data to countries outside the EU.

We appreciate the opportunity to comment on the Guidelines for transfers of personal data between EEA and non-EEA public authorities and bodies.

ISBER HEAD OFFICE • 750 West Pender Street – Suite 301, Vancouver BC V6C 2T7, Canada | T 604.484.5693 | F 604.874.4378 • www.isber.org

General Comments:

The document is intended to provide guidance on transfers of personal data from EEA public authorities or bodies ("public bodies") to public bodies in third countries or to international organizations when these are not covered by an adequacy finding adopted by the European Commission. The document cites as one example, US public bodies which are not covered by the EU-US Privacy Shield, which only applies to private sector organizations. However, it would be helpful to further clarify the distinction between "public bodies" and "private bodies" and provide additional examples, if possible.

Specific Comments:

p. 6., 2.2, Definitions, item #13. This recommendation suggests that international agreements should contain definitions of the basic personal data concepts in line with the GDPR relevant to the agreement in question. A number of examples of important definitions are provided in this section. We strongly suggest that the terms 'anonymisation' and 'pseudonymisation' be included in the examples of important definitions because these terms are often not defined or used consistently in the research community and their definitions vary among (and sometimes even within) different jurisdictions across the globe. We strongly recommend that clarification be provided that pseudonymized data may be considered anonymized when in the hands of an entity that does not possess the keycode required to reidentify such data; and that appropriate measures are put in place to prevent the holder of the data from gaining access to the keycode or otherwise linking the data set to other data sources that may permit re-identification. For example, such measures could be included in the international agreement by stipulating that the identities of the data subjects will not be disclosed and no attempts will be made to re-identify them. Such agreements are a best practice that is currently frequently used by biobanks and research teams for protecting the privacy and confidentiality of subjects.

p.6., 2.3.1, Purpose limitation principle, item #15. It is stated that international agreements need to specify the purposes for which personal data is to be transferred and processed. However, it is not clear how specific the purposes must be detailed. Additional guidance would be helpful.

p.7., 2.3.2, Data accuracy and minimisation principles, item #19. It is stated that the data minimisation is important to avoid the transfer of personal data when they are "inadequate or excessive." It is not clear what is meant by being "inadequate or excessive." Would it be possible to further clarify this point?

p.7., 2.3.3, Storage limitation principle, item, #21. This is a very helpful indication and for specific projects and data exchanges this is entirely applicable. However, it would be useful to have guidance with regard to data exchanges that produce publishable results that require

ISBER HEAD OFFICE • 750 West Pender Street – Suite 301, Vancouver BC V6C 2T7, Canada | T 604.484.5693 | F 604.874.4378 • www.isber.org

individual data to be placed in a publicly available database. Furthermore, international initiatives that share important genomic information with the international scientific community would struggle to commit to the minimization and storage limitation principle while following the guiding FAIR data principles, making data Findable, Accessible, Interoperable and Reusable to advance public health discoveries. Including FAIR principles in the guidance would be helpful.

p.8., 2.3.4, Security and confidentiality of the data, item #23. This guideline recommends that the notification timeline for a personal data breach, as well as procedures for communication to the data subject, be defined in the international agreement. However, it should be recognized that if the personal data concerns anonymized genetic data alone (without links to personal identities), it would not be possible to notify data subjects of a breach. Furthermore, in the case of pseudonymized data, the possibility of the data receiver being able to advise the Supervisory Authority and individual data subjects through the transferring third party pursuant to Article 33 and Article 34 could be impractical. Confirmation that the supervisory authority in such a scenario pursuant to Article 34 would be the Supervisory Authority of the transferring public research entity. It would also be helpful to clarify, in this instance, what constitutes a "data breach" and whether, for pseudonymized data, only relinking to the code would be considered a data breach.

p.8., 2.4.1, Right to transparency, item #28. It would be helpful to provide some examples of appropriate redress mechanisms.

p.9., 2.4.1, Right to transparency, item #30. This recommendation states that the parties of the international agreement must commit to make the agreement available to data subjects on request and to make the international agreement or the relevant provisions providing for appropriate safeguards publicly available on their website. This seems overly prescriptive, particularly in the context of biobanking, and may not reach the intended goal of the recommendation. The requirement for both parties of an international agreement to publish every single agreement document and the provisions for providing appropriate safeguards would require extensive effort and resources and, in many cases, with little benefit to the data subject. In many cases, the data subject would not know which study was accessing their data or which agreement was relevant to sharing of their data. Thus, this recommendation may not accomplish the intended objective.

p.9., 2.4.1, Right to transparency, item #28 - #30. There is some contradiction in these items with regard to the requirements of a general information notice. While #28 requires a general information notice as a minimum requirement but specifies that the use of a website is not considered sufficient, #30 indicates that the website is sufficient for the publication of appropriate safeguards. Some clarification would be useful.

Furthermore, the requirement to provide individual information to each data subject could potentially create an impossible administrative burden for the public research entity. While this

ISBER HEAD OFFICE • 750 West Pender Street – Suite 301, Vancouver BC V6C 2T7, Canada | T 604.484.5693 | F 604.874.4378 • www.isber.org

should not be a reason for noncompliance with the regulation, it would be useful for the EDPB to consider the implications and provide mechanisms that are feasible without unduly hindering important research. This requirement may not meet its intended goal of reaching the relevant data subjects. We recommend that a general information notice on the website of the public body be considered sufficient as it is for the publication of appropriate safeguards.

Finally Article 14 (5) (b) provides the exception for scientific research subject to the conditions and safeguards referred to in Article 89 (1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available. Here as in Article 13, there is reference to the appropriate safeguards so further elucidation would be helpful on this point.

p.9., 2.4.2, Rights of access, to rectification, erasure, restriction of processing and to object.

It is admirable that data subjects right to access all data pertaining to them is protected and guaranteed even within a research context as indicated in points 31 to 33. That said, the timelines presented for the response of these requests should be contextualized for large initiatives such as the 1million genomes project and larger international consortia such as ICGC-ARGO in which many Europeans will contribute. Once again, the scientific value of these international data bases and their ability to further scientific analysis and produce results that have a clinical impact need to be balanced against the guidelines for international data transfers and access and how potentially the exceptions indicated as per point 35 under Article 17 (3).

It is also important that terms such as "manifestly unfounded" and "excessive" be given some definition and some boundaries be provided, in order not to be abused.

p.10.,2.5, Restrictions on onward transfers and sharing of data, item #38. It is appreciated that onward transfers are addressed. This is a point that material and data transfer agreements used for scientific research has always addressed and it is important that this clarification has been reported here in the guidelines. In fact, point 38 addresses the issue of purpose limitation and commitment to provide the same protection as per the original agreement if in fact the agreement permits onward transfers. Under normal circumstances these onward transfers must be agreed with the original provider of the data as the first and main controller and this should be emphasized in the guideline.

p.11., 2.7, Redress Mechanisms, item #46. The reference here seems incorrect for the section on supervision mechanism is section 2.8 not section 8.

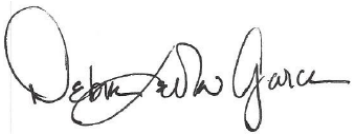
p.11., 2.7, Redress Mechanisms, item #48. The issue of judicial remedy remains the main issue in terms of international agreements with public bodies as addressed in point 47 and point 48.

ISBER HEAD OFFICE • 750 West Pender Street – Suite 301, Vancouver BC V6C 2T7, Canada | T 604.484.5693 | F 604.874.4378 • www.isber.org

While it is understandable that the transferring body has the first responsibility to how the personal data are managed and transferred, it would be unreasonable for them to sustain the entirety of the burden and therefore the guideline should also include the mechanisms for the burden to be shared or for the transferring body to have judicial redress or quasi-judicial redress to the receiving body. It is important to note that the mechanisms must be such that they do not inhibit the ability for the public bodies to share data due to exaggerated resolution mechanisms.

Thank you for your consideration of these comments.

Respectfully submitted,



Debra Garcia
ISBER President
May 15, 2020

ISBER HEAD OFFICE • 750 West Pender Street – Suite 301, Vancouver BC V6C 2T7, Canada | T 604.484.5693 | F 604.874.4378 • www.isber.org