Comments of the World Privacy Forum to
The European Data Protection Board

Regarding

R01/2020, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*

20 December 2020

Dear Members of the European Data Protection Board,

Thank you for the opportunity to provide feedback on *Recommendations 01/2020* on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, published 11 November 2020 at https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en. The World Privacy Forum supports the stated goals of the Recommendations to facilitate "the free flow of personal data within the European Union, while preserving the fundamental rights and freedoms of individuals, in particular their right to the protection of personal data." However, we also have concerns about the Recommendations, which we discuss in these comments.

The World Privacy Forum is a non-profit, public interest research group. We are non-partisan, and we focus on conducting in-depth research and analysis regarding privacy. Much of our work since 2002 has focused on data ecosystems and privacy. (See, for example, our peer-reviewed research on India's Aadhaar biometric ecosystem, *A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, Pam Dixon, Springer Nature, Health Technology. DOI 10.1007/s12553–017-0202-6. http://rdcu.be/tsWv.) In 2020, we have been researching the impact of COVID-19 on privacy across key international jurisdictions. We also have published, jointly with the Center for Global Development, a scoping research paper on COVID-19 impacts in Low and Middle Income Countries (LMICs) (See, Michael Pisa, Pam Dixon et al, *Governing Data for Development, Trends Challenges and Opportunities*, https://www.worldprivacyforum.org/2020/11/governing-data-for-development-trends-challenges-and-opportunities/.) Also this year, WPF served on the World Health Organization's health data privacy policy board. More information and publication are available at www.worldprivacyforum.org.

In reading the Recommendations, we found several areas which, if improved, would enhance the stated goals of the EDPB for facilitating free flow of data while preserving fundamental rights and freedoms of individuals, including the right to protection of personal data. As noted earlier, we also have some concerns regarding the language in the current Recommendations

which could have negative impacts on both data flows and privacy. We discuss our concerns below.

I. Addressing the challenges of complex data ecosystems

Even in the relatively brief amount time that has passed since the GDPR was negotiated, data ecosystems have measurably and observably become more complex. Today's data transfers can be characterized and understood not just as "data transfers" as such, but also as transfers between and amongst one or more, even myriad, complex data ecosystems. These ecosystems exist not just within the EU, but globally — and these data flows and ecosystems are often, and increasingly, inextricably entwined. The current draft of the Recommendations does not address this issue directly enough. Adding a broader understanding to the Recommendations pertaining to ecosystem complexity and what it means regarding implementation would allow the Recommendations to be more compatible with modern data ecosystems and the practical operations and data flows amongst and between these ecosystems, and would ultimately facilitate better data protections for Europeans and others. We acknowledge that data mapping is a key tool. But data mapping does not always capture the full complexity and context of the ecosystems, and can fall short of addressing actual risks, as well as something we call "data entanglement."

In studying data ecosystems, we have documented that ecosystems can become irretrievably entangled. COVID-19 data ecosystems, as well as some global financial ecosystems, which we discuss below, are examples of this. Another type of data ecosystem that can be deeply and often irretrievably entangled are identity ecosystems, which are often layered and function simultaneously, which operating sometimes separately, sometimes overlapping. (See *Digital Identity Ecosystems*, https://www.worldprivacyforum.org/2019/02/digital-identity-ecosystems/ .) Our recent presentation on data entanglement for the National Academy of Sciences, Engineering and Medicine will provide further background on this topic, including privacy implications. (See, *Looking Ten Years Ahead: Key Converging Technologies in Computing, Data, and Analysis and the Implications for Governance, Standards, and Norms in Knowledge and Privacy*, https://www.nationalacademies.org/event/10-28-2020/the-future-of-data-science.) Without going into arcane detail about data entanglement, in short, it impacts data transfers in meaningful ways, creating inabilities to genuinely disentangle specific data elements and sometimes even categories of data elements from certain data ecosystems. These data ecosystems do not have neat and tidy lines, and they overlap each other, often across multiple jurisdictions. We note that moving forward, it will be increasingly rare to see EU-only data ecosystems, as ecosystems may readily be situated across borders.

Here, we point out several exemplars pertaining to data system complexity and entanglement in relation to Use Case 7, *Remote access to data for business purposes*, which can in some cases also have impacts related to Use Case 6, *Transfer to cloud services providers or other processors which require access to data in the clear.*

The Recommendations, Use Case 7 states:

> A data exporter makes personal data available to entities in a third country to be used for shared business purposes. A typical constellation may consist of a controller or processor established on the territory of a Member State transferring personal data to a controller or processor in a third country belonging to the same group of undertakings, or group of enterprises engaged in a joint economic activity. The data importer may, for example, use the data it receives to provide personnel services for the data exporter for which it needs human resources data, or to communicate with customers of the data exporter who live in the European Union by phone or email.

If
1. a data exporter transfers personal data to a data importer in a third country by making it available in a commonly used information system in a way that allows the importer direct access of data of its own choice, or by transferring it directly, individually or in bulk, through use of a communication service,
2. the importer uses the data in the clear for its own purposes,
3. the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society, then the EDPB is incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights.

We appreciate the intent here. We offer two exemplars of how despite the best intent, this recommendation is not feasible in practice, and the recommendation does not adequately take into account ecosystem complexity nor ecosystem context.

Exemplar: COVID-19-related data transfers

The COVID-19 pandemic has brought new challenges to data protection and privacy in many jurisdictions, including the U.S. We have written in detail about how the waiving of selected elements of the U.S. sectoral health data protection law, HIPAA, during the pandemic has had a deleterious impact, generally, on certain sensitive privacy concerns. (See Robert Gellman and Pam Dixon, *COVID-19 and HIPAA, HHS's Troubled Approach to Waiving Privacy and Security Rules for the Pandemic*, https://www.worldprivacyforum.org/2020/09/covid-19-and-hipaa/.) In our research for this work, in our work with the WHO, and in our research and interviews for the joint WPF/CGDEV report, we have seen and discussed how some of the key pandemic health data flows are mapping and working.

At this point in time, large amounts of health-related data flowing in highly complex data ecosystems are being transferred across jurisdictions and into multiple, sometimes intersecting ecosystems. Because these transfers are occurring from many global jurisdictions to, for example, the WHO and to other public health bodies, Use Case 7 comes into play, as does Use Case 6 in some instances. Because of the pandemic, health data transfers may well and often do include microdata. This data has been used to understand the pandemic, and has been used to save lives and conduct research and facilitate cooperation across borders. Although we have concerns about this increased flow of health microdata, we also understand that saving lives must come first, and that the data flows are essential.

For more detail on types of COVID-19 data ecosystems, see, for example, the WHO COVID-19 Dashboard https://covid19.who.int, Singapore's COVID-19 dashboard https://co.vid19.sg/singapore/ , and for a detailed look at the more technical datasets, see Next Strain, https://nextstrain.org/sars-cov-2/, in particular the *Genomic epidemiology of novel coronavirus - Global subsampling,* which samples 3,470 genomes sampled between Dec. 2019 and Dec. 2020, https://nextstrain.org/ncov/global.

Regarding the Recommendations, it is unclear to us how entities sharing pandemic-related data across borders may comply with Use Case 7 or Use Case 6 in all instances. Encryption as a safeguard will not apply with some COVID-19 data transfers, because in this context, the data can appear in unencrypted form in third countries, including those without EU adequacy.

We note that the Recommendations appear to require data localization in some cases, which we find to be an objectionable requirement that is both impractical and damaging to privacy. Data localization will stifle the very data flows that have facilitated global coordination on COVID-19. We urge the EDPB to address COVID-19-related and similar transfers by taking a

more detailed and broad analysis of the details of how these transfers take place with multiple stakeholders across multiple jurisdictions.

The Court's ruling in *Schrems II (*Case C-311/18, 2020) has been broadly interpreted thus far as facilitating compliance approaches that utilize an analysis based on the actual level of risk that a non-EU government will demand access to data, in particular personal data. The EDPB Recommendations do not appear to allow this same analysis, which in turn creates a new risk, which is that transfers based on Standard Contractual Clauses appear to be further restricted, apparently limiting their use to a slim number of situations. This approach makes untangling the compliance issues with crucially important and complex data ecosystems such as are present in the COVID-19 context extremely difficult, if not impossible to parse. We further note that the Recommendations appear to require data localization, which we find to be a negative precedent. If this was not the intent of the EDPB, then the language needs to be clarified.

Currently, Use Cases 6 and 7 are likely to impact COVID-19 data transfers, given that many data transfers regarding COVID-19 are occurring from many parts of the health ecosystem and the world, and further, may be originating in part from businesses and organizations that do not fall into easily categorizable public health entities. We agree that this is a complex problem. It deserves more attention and detailed documentation. The details matter, and if the conclusions of the Use Cases 6 and 7 are not amended, then it is likely that a range of meaningful COVID-19 data transfers may cease. Some will likely pass through, but not all, and perhaps not even most.

Additionally, we note that there is no acknowledgement of data transfers in regards to multilateral institutions in the Recommendations (We note p. 38 discusses the UN, but the focus is the UN as a resource for reports and resolutions.) We understand the reasons for this broad omission, however, we question the wisdom of ignoring the topic of multilateral data transfers and urge the EDPB to consider engaging with multilateral institutions given how centrally important they are becoming to personal data transfers. Multilateral organizations hold extremely detailed microdata. See, for example, UNHCR's Socio-economic impact of COVID-19 on refugees in Kenya, 2020, which contains microdata, https://microdata.unhcr.org/index.php/catalog/245#metadata-data_access.

We understand there is not a legal basis for compelling cooperation, however, it is important that a voluntary, cooperative dialogue is begun. We have already mentioned COVID-19 data transfers to and from, for example, the WHO and other relevant entities. European data pertaining to RoHS and REACH regarding toxic chemical safety is also monitored by multilateral organizations. While the REACH and RoHS data generally does not contain microdata, the broader pattern of data transfer amongst multilateral organizations is a well-understood one, and patterns of transfers of personal data transfers to multilateral organizations is likely to continue. The EU should not simply ignore this, but rather seek dialogue.

It would be beneficial for the use cases articulated in the Recommendations to specifically analyze and groundtruth COVID-19 and other data transfers and to understand at a granular level how they may happen, and what mitigations may be possible. It is not sufficient to broadly state that transfers such as described in Use Case 6 and 7 are not feasible, because these transfers are going to continue to occur in multiple scenarios.

Exemplar: Financial sector data ecosystems and transfers

In the financial sector, high-velocity, high-volume data transfers occur routinely. We bring to your attention one exemplar of such transfers, which is the significant FINRA data ecosystem, which intersects with other global ecosystems. These complex transfers could well be included under both Use Case 6 and 7, depending on the analysis. It is unlikely that the EU would desire a stoppage to such transfers.

By way of background, FINRA, the Financial Industry Regulatory Authority, is a self-regulatory organization under the Securities and Exchange Act ('34 Act). It is authorized by the U.S. Congress to issue rules under Section 15A(b)(6) of the '34 Act in order to "…prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, and, in general, to protect investors and the public interest and Section 15A(b)(9) of the Act." FINRA's activities began in a paper-based world. By the 2000s, financial market regulators such as the SEC and FINRA were developing the capacity to collect and analyze raw data feeds directly from regulated entities. This brings us to today, where FINRA is using the availability of increased technological capacity to acquire real-time transaction data regarding TRACE - eligible securities (Trade Reporting and Compliance Engine). Instead of receiving periodic reports, those subscribing to FINRA's TRACE reporting system now have firehoses of real time data to manage and analyze — by last count in December 2020, FINRA processes more than 67 billion electronic records per day.

In 2011, the Depository Trust & Clearing Corporation (DTCC) and the Society for Worldwide Financial Telecommunications (SWIFT) launched a collaborative, global standard-setting effort that led to the creation of the "Global Legal Entity Identifier" standard. This standard has been endorsed by the Financial Stability Board and the G20 and was designated as International Organization for Standardization ISO standard 17442. Some jurisdictions outside the United States have begun mandating the use of LEI numbers in certain financial service markets in order to increase the effectiveness of regulatory oversight processes (e.g., EU Markets in Financial Instruments Directive known as MiFID II).

Any legal entity anywhere in the world can obtain quickly, easily and cheaply a globally unique 20 digit LEI number from the LEI issuer of their choice, and be confident that it will be accepted by regulators and counter-parties around the world for compliance purposes. (See https://www.gleif.org/en/.) The LEI Regulatory Oversight Council and the Global Legal Identifier Foundation (GLEIF) jointly administer the LEI system. This includes the oversight of a global network LEI issuers that compete with each other to issue LEI numbers to entities; providing the Global LEI Index, an open, searchable database of LEI numbers, and monitoring emerging technologies and updating the standard as needed to accommodate them.

This is a complex, global, and real-time to near real-time data ecosystem. Currently, FINRA has entered into information-sharing memorandums of understanding (MoUs) with key foreign regulators to "...allow for collaboration and coordination on selected issues. Through these MoUs, FINRA can work with foreign counterparts to investigate possible instances of cross-border market abuse in a timely manner, exchange information on firms under common supervision of both regulators, and allow for coordination on supervision of firms and markets." FINRA is not a U.S. government agency, it is an NGO.

FINRA currently has MoUs to share regulatory information with France, the Netherlands, Spain, and other jurisdictions. The Recommendation's Use Cases 6 and 7, when analyzed against this complex data ecosystem, does not properly parse. The financial data, to be analyzed and utilized by all global stakeholders, will be accessed on shared systems, or in other ways that are out of bounds according to the Recommendations. Standard Contractual Clauses appear to largely be taken off of the table as a possibility for mitigation. FINRA is but one example of an entangled global ecosystem that would be extremely difficult if not entirely impossible to adjudicate by following the Use Cases and Recommendations as currently written. Because it

is unlikely that the EU would want to simply invalidate the existing MoUs and, depending on the analysis, remove its participation in SWIFT, FINRA, LEI ROC and GLEIF, the Recommendations will need to be changed to reflect the reality of this complexity.

In its decision, the Court in *Schrems II* adjured those wanting to export data to consider the full context of a transfer(s) when evaluating the legality of the transfer(s). See ¶¶121 and 146, and ¶134. The Court stated that transfers should be analyzed "in the light of all the circumstances of that transfer" and "on a case-by-case basis." Given this basis, an analysis that allows for the MoUs with France, the Netherlands, and Spain could be sustained. Also sustainable in many cases will be COVID-19 transfers using this analysis. We urge the EDPB to include the Court's approach to assist with complex data ecosystems.

II. Addressing Low and Middle Income Countries and Small and Medium Enterprises

While this topic is not directly addressed in the Recommendations, we are nevertheless concerned about the impact of these Recommendations on LMICs and SMEs. While wealthy jurisdictions such as the EU have more resources, infrastructure, skilled workers, and resilience to adapt to some parts of the Recommendations, companies located in the less wealthy countries, many of whom are impacted deeply by the pandemic, do not always have the resiliency to adopt these Recommendations. The same is true of many small and medium sized enterprises (SMEs) which have globally also been negatively impacted by the pandemic and may not have access to legal, technical, and administrative assistance in attempting to comply with the language of the Recommendations.

To achieve the stated goals of the EDPB, the Recommendations need to provide a stable and consistent base upon which a variety of jurisdictions, and the businesses within them, can rely. We are concerned about the EDPB's Recommendations regarding the apparent requirements for data localization, as well as the language that appears to curtail uses for standard contractual clauses in context. These Recommendations, should they go forward, such as mandatory data localization, and removal of a key compliance tool, will lead to less, not more privacy.

It is our hope that the EDPB will take more broadly into consideration the needs of LMIC jurisdictions, particularly those which have passed GDPR-like data protection laws, and support their efforts by including the ability to utilize a case -by- case analyses as discussed by the Court that can potentially enable more jurisdictions to move into compliance.

III. Conclusion

Thank you again for the opportunity to provide feedback on the Recommendations. We appreciate the opportunity, and would welcome further conversation with you about these topics.

Sincere regards,

Pam Dixon
Founder and Executive Director
World Privacy Forum
www.worldprivacyforum.org