ICANN org Comments on the Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance With the EU Level of Protection of Personal Data

1. About the Internet Corporation for Assigned Names and Numbers (ICANN)

The Internet Corporation for Assigned Names and Numbers (ICANN) is a not-for-profit public-benefit corporation that, on behalf of the Internet community, oversees the technical coordination of the top-most level of the Internet's Domain Name System (DNS), and especially its security, stability, and resiliency.

ICANN brings together governments, non-commercial and commercial stakeholder groups, civil society, and individuals. Each group represents a different interest on the Internet. Collectively, they make up the ICANN community, which develops policies for the DNS through a consensus-driven bottom-up process.

2. ICANN Working to Create GDPR-Compliant Data Access System

The requirements of the EU General Data Protection Regulation (GDPR) have had a significant impact on the personal data processing activities of the whole Internet community. This includes the transfer of personal data from third parties to and within the ICANN organization ("**ICANN org**"). ICANN org is headquartered in Los Angeles and has regional offices in Brussels, Istanbul, Montevideo, and Singapore. ICANN org also has engagement centers in Washington, D.C., Geneva, Beijing, and Nairobi. As a consequence, ICANN org undertakes necessarily a number of international data transfers subject to Chapter V requirements of the GDPR.

ICANN org and the ICANN community are currently working closely to develop a new System for Standardized Access/Disclosure ("**SSAD**") for gTLD registration data, which would facilitate access to non-public generic top-level domain ("**gTLD**") registration data for parties with a legitimate interest in accessing that data, in furtherance of the global public interest. Before the GDPR came into force, personal data relating to gTLD registrants could, in principle, be publicly accessed by anyone through a simple search form without any further limitation or control. With the full applicability of the GDPR, however, existing public databases were redacted, thus requiring a more case-specific approach. The European Commission has called the work to develop such a standardized access/disclosure system "*vital and urgent*" and urged ICANN org to expeditiously address this issue. The Commission wrote in a 3 May 2019 letter to ICANN org that "*the current situation where access to non-public registration data for public policy objectives is left at the discretion of registries and registrars affects the EU Member States authorities' ability to obtain legitimate access to non-public registration data necessary to enforce the law online, including in relation to the fight against cybercrime."*

The recently proposed SSAD model would change the current fragmented state by introducing a centralized process for managing access requests and placing ICANN org in the middle of this process. ICANN org or its designee(s) would manage a system for the intake of requests for data and would route these requests to the registrar or registry operator for a response. This new system would introduce a significant volume of new processing of requestors' data, including personal data, by ICANN org and/or its designees. This system is, by its very nature, inconceivable without allowing international data transfers to the extent necessary. Such transfers would be necessary, *inter alia*, to rapidly verify and automatically process lawful requests from law enforcement authorities. The SSAD is therefore instrumental for stopping and preventing the dissemination of illegal content and in order to avoid related societal harms. Considering the current version of the Recommendations and its strict interpretation of the GDPR's international data transfer requirements, these efforts are fundamentally at stake — also to the detriment of data subjects.

As noted in ICANN org's 10 December 2020 comments to the European Commission concerning the draft updated Standard Contractual Clauses, a risk-based approach lies at the heart of this effort. As explained in greater detail below, ICANN org believes that this necessary aspect is critically absent in the European Data Protection Board's (**"EDPB**") Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the "**Recommendations**") and encourages the EDPB to introduce this approach in the Recommendations.

3. Putting Critical International Data Transfers at Risk (Use Cases 6 and 7)

While ICANN org generally welcomes the intention of the EDPB to provide further guidance for organizations engaged in international data transfers following the invalidation of the EU-US Privacy Shield in the *Schrems II* decision of the Court of Justice of the European Union ("**CJEU**"), ICANN org remains concerned that the EDPB adopted a rather strict interpretation of the *Schrems II* decision resulting in the need to either radically suspend data transfers for a variety of legitimate critical purposes or continue with these transfers in a regulatory "grey zone."

ICANN org's concerns in this regard relate in particular to the Use Cases 6 (Transfer to cloud services providers or other processors which require access to data in the clear) and 7 (Remote access to data for business purposes), for which the Recommendations note that no *effective* supplementary *technical* measures could be found to ensure an essentially equivalent level of protection for the data transferred to a third country.

The Recommendations suggest that contractual or organizational measures are considered *non-effective* in this situation, s*ee*, Paragraph 48 of the Recommendations:

"*Contractual and organisational measures alone will generally not overcome access to personal data by public authorities of the third country (where this unjustifiably interferes with the data importer's obligations to ensure essential equivalence). Indeed, there will be situations where only technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes*"; and

Paragraph 95 of the Recommendations:

"*As said, contractual measures will not be able to rule out the application of the legislation of a third country which does not meet the EDPB European Essential Guarantees standard in those cases in which the legislation obliges importers to comply with the orders to disclose data they receive from public authorities*".

As a result, data exporters would have to refrain from starting such data transfers. If they are already conducting such transfers, they would be required to suspend or end the transfer of personal data. When applied in the ICANN context, this recommendation could lead gTLD registrars and registry operators to cease transferring registration data to recipients in many jurisdictions globally under any circumstances. This could potentially affect transfers from registry operators to registrars for the purpose of setting up a domain, to escrow agents, to DNS servers or to ICANN org for compliance inquiries. This could also affect transfers in response to access requests (including those in the context of the SSAD proposed), irrespective of the legitimate interests of third parties from the private and the public sector alike underlying these transfers. Third parties in both the private and public sector may pursue legitimate interests in accessing registration data for a variety of purposes and important objectives of general public interest, such as public security, (cyber) crime prevention and investigation, or the enforcement of civil law claims (*see*, Article 23(1) GDPR). *See* also, Paragraph 52 of the Recommendations. Hampering international transfers of personal data that are necessary within the ICANN and the Internet ecosystem will create severe security and stability risks for the Internet.

4. <u>Omitting the Possibility of a Risk-Based Approach</u>

ICANN org believes that this very strict understanding set out in the EDPB's Recommendations, omits the possibility of a risk-based approach, which has been enshrined in the GDPR (notably in Art. 35 GDPR). ICANN org would like to stress that a view not fully reflecting the conflicting interests in ensuring a high level of protection of personal data while requiring practically manageable transfer impact assessments does not echo the flexibility provided by the GDPR (*see*, A. below) and conflicts with ongoing legislative developments (*see*, B. below).

A. The GDPR's Inherent Risk-Based Approach Applies to Third Country Data Transfers

The risk-based approach is firmly established in EU primary law and case law. Both of them have since the beginning been based on the principle of proportionality which does not recognize a supremacy of specific fundamental rights, but instead strives for their equitable balance in each case. S*ee*, Article 52(1), sentence 2 of the EU Charter of Fundamental Rights, which also contains the freedom of expression and information (Article 11), the freedom to conduct a business (Article 16), and the right to property (Article 17). These legal positions are not mentioned at any point in the Recommendations.

As a result, protecting data subjects is restricted by the Recommendations to *preventing* data transfers instead of considering the legal positions and public interests that speak *in favor* of such transfers, which may well be pursued in the very interests of data subjects (*see*, 3. above).

More specifically and in no way any less significant, the GDPR embraces the concept of risk-based assessments, as is obvious from Articles 24(1), 25(1), 27(2)(a), 30(5), 32(1) and (2), 33, 34, 35, 36, 39(2), 49(1)(a) of the GDPR and numerous recitals, with recital 75 leading the way, expressly referring to the "*rights and freedoms of natural persons*." In addition, the GDPR's Chapter V provisions on transfers of personal data to third countries or international organizations acknowledge the risk-based approach in multiple ways.

First, the GDPR allows data subjects to waive further protection by giving informed consent to the transfer under Article 49(1), sentence 1, letter a GDPR. The general possibility of granting consent has already been acknowledged in Article 8(2), sentence 1 of the EU Charter of Fundamental Rights (the "**Charter**"). Any personal data transfer to third countries without an adequacy decision pursuant to Article 45 GDPR or appropriate safeguards pursuant to Article 46 GDPR can thus take place if the data subject, prior to giving consent, was properly "*informed of the possible risks of such transfers.*"

Second, Article 49(1), Subparagraph 2 GDPR has introduced a new risk-based derogation that was not previously included in the former Directive 95/46/EC:

"Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection

of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued."

This derogation is restricted to non-repetitive transfers concerning only a limited number of data subjects and requires the application of "suitable" (instead of "appropriate") safeguards, to be determined on the basis of an assessment by the data exporter of all circumstances surrounding the data transfer, along with a specific "necessity test" to ascertain "compelling legitimate interests" by the data exporter. Considering its limited scope of application, the EDPB deems this derogation to be a "last resort" only.[1] In light of the judgment C-311/18 (*Schrems II*) of the CJEU, however, one might consider interpreting the scope of application of this provision more generously. The CJEU noted by emphasizing the permission, not the prohibition, of third country data transfers:

"[…] *in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR.*"

Recital 113 of the GDPR points for the assessment to be undertaken by the data exporter of "*all the circumstances surrounding the data transfer"* to certain elements that overlap with the proposed (non-exhaustive) list of factors set out in Paragraph 49 of the Recommendations and also in "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures." All sources mentioned target the same line of protection by considering, *inter alia*, the nature of the personal data, the transfer's purpose and duration as well as the situation in the country of origin, the third country, and the country of final destination. However, since the additional requirement to inform the competent supervisory authority prior to any transfer based upon the above-mentioned risk-based derogation would, if used more frequently, most likely generate an untraceable flood of notifications with individual risk assessments hardly consistent in scope and depth, it seems more appropriate to distinguish recurring risk-specific Use Cases (*see*, 5. below) by the EDPB.

B. Contradiction With New Legislative Acts Introduced by EU Commission

This position appears to be in conflict with the new draft Standard Contractual Clauses proposed by the European Commission, which mandate a risk-based approach. *See*, clause 2 (b) (i):

[1] See, EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, p. 14.

"The Parties declare that in providing the warranty in paragraph a, they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the content and duration of the contract; the scale and regularity of transfers; the length of the processing chain, the number of actors involved and the transmission channels used; the type of recipient; the purpose of processing; the nature of the personal data transferred; any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred; …".

Similarly, the existing Standard Contractual Clauses (Processors) refer to requirements imposed on the data importer (emphasis added) "*to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses*" (*see*, Article 4) in the context of the power of authorizing data protection authorities "*to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data.*" Therefore, also the existing Standard Contractual Clauses regard the *likelihood* of access to the personal data transferred in the country of the data importer to be a relevant factor to be considered.

Nevertheless, Paragraph 42 of the Recommendations states (emphasis added):

"*Your assessment must be based first and foremost on legislation publicly available. However, in some situations this will not suffice because the legislation in the third countries may be lacking. In this case, if you still wish to envisage the transfer, you should look into other relevant and objective factors, and not rely on subjective ones such as the likelihood of public authorities' access to your data in a manner not in line with EU standards*."

This statement seems surprising, as the likelihood of access to data is a factor that can also be considered on an objective basis (*e.g.*, by looking at the numbers of access requests received and the percentage of requests answered positively), which is, as mentioned in the foregoing, an approach expressly mandated under the new draft Standard Contractual Clauses proposed by the European Commission.

Furthermore, the Recommendations shift the burden of assessment on "essentially equivalent" (or inequivalent) third country laws and practices considerably to the data exporter, while data importers would only need to collaborate "*where appropriate*." However, and quite understandably, the new draft Standard Contractual Clauses proposed by the European Commission emphasize the role of data importers in carrying out such assessments (*see*, Annex,

Section II, Clause 2, letter c), expressly requiring data importers to warrant that they have undertaken "*best efforts*" in providing the data exporter with relevant information. In global multi-actor processing chains, only such a commitment from data importers could ensure that the intended high level of data protection can be attained and maintained in the long term.

ICANN org, which collaborates with gTLD registrars and registry operators, data escrow agents, and dispute-resolution service providers from almost all jurisdictions at the most diverse stages of development in terms of data protection regimes and international commitments (*e.g.*, adherence to the 2013 OECD Guidelines on Data Protection or the CoE Convention 108+), therefore suggests to put an emphasis on involving data importers to a greater extent in order to draw on their existing knowledge of local laws and practices.

5. Introducing the Risk-Based Approach

In order to provide organizations engaged in international data transfers with more certainty and flexibility, ICANN org regards it as critical to introduce the risk-based approach expressly in the Recommendations. The EDPB should consider in this context to develop Use Cases for high-risk situations where it would be necessary to implement the technical measures suggested in the Recommendations (and which "*might impede or render ineffective access by public authorities in third countries,*" *see*, Paragraph 48 of the Recommendations). For situations that present low risks for data subjects, organizational and/or contractual measures might suffice.

6. Closing Remarks

The issues addressed in this comment are critical, including to the work of ICANN org and the ICANN community to develop a system for standardized access/disclosure of non-public gTLD registration data in compliance with the GDPR (the SSAD), and other activities essential for the Internet's ecosystem, including registering domain names, transfers of registration data from registrars to registries, and transfers to escrow agents. To maintain and further guarantee a level of protection of personal data to which all EU and non-EU stakeholders can effectively and reasonably aspire, we would appreciate it if the above considerations could please be taken into account by the EDPB.

* * *