

August 3, 2018

VIA E-MAIL

Göran Marby
Chief Executive Officer and President
Internet Corporation for Assigned Names and Numbers
Contact Information Redacted

Re: **Proposed Model for a Centralized RDDS System Managed by ICANN**

Dear Göran,

Thank you again to you and John for making time to continue discussions regarding the proposal for the centralized management of WhoIs information and provision of access to non-public WhoIs data by ICANN.

As we discussed, ICANN's expressed interest in finding a way to be legally responsible for the handling of WhoIs data, and to reduce the legal responsibility of the contacted parties for such with respect to GDPR supports at least the serious consideration of this model by ICANN, if not its adoption. You have expressed this goal publicly on several occasions, most recently at the IPC Open Session during ICANN 62.¹ You have also expressed concern that transfer of WhoIs information from contracted parties to ICANN may be problematic under GDPR.

During our last conversation I told you that I was confident that if structured properly that the proposed model would accomplish this expressed goal of ICANN and result in full legal responsibility for ICANN for managing requests for access to non-public information and reduced or eliminated liability for contacted parties with respect to requests for access to non-public information, while not running afoul of GDPR and other laws regulating the transfer of personal data outside of the EU. I also committed to you to consult with legal counsel with expertise in EU privacy law to confirm that this model is consistent with GDPR and to provide a more specific legal basis in support of the model.

Since then, I have done just that, with assistance from Flip Petillion, Alexander Heirwegh and Jan Janssen at PETILLION. In preparation for our call next week, please find below a summary of the legal bases in support of the proposed model with a more detailed

¹ See, e.g., ICANN Transcription ICANN Panama City GNSO IPC Open Meeting Tuesday, 26 June 2018 at 12:15 EST, Pg. 9 (“We actually have been trying to, together with the European Commission, and I've said this openly, to make ICANN Org legally responsible for the handling of the data because I think we actually have a moral responsibility as an organization to be legally responsible because we are actually mandating to contracted parties to collect the data. So far we haven't been able - no one has been able to put that in front of being legally responsible for GDPR. And that means that the notion of a unified access model which actually puts on top of all the contracted parties has to contain something that takes away some legal responsibility from them.”)

ALBANY
AMSTERDAM
ATLANTA
AUSTIN
BOSTON
CHICAGO
DALLAS
DELAWARE
DENVER
FORT LAUDERDALE
HOUSTON
LAS VEGAS
LONDON*
LOS ANGELES
MEXICO CITY*
MIAMI
MILAN**
NEW JERSEY
NEW YORK
NORTHERN VIRGINIA
ORANGE COUNTY
ORLANDO
PALM BEACH COUNTY
PHILADELPHIA
PHOENIX
ROME**
SACRAMENTO
SAN FRANCISCO
SEOUL*
SHANGHAI
SILICON VALLEY
TALLAHASSEE
TAMPA
TEL AVIV*
WARSAW~
WASHINGTON, D.C.
WHITE PLAINS
* OPERATES AS GREENBERG
TRAURIG MAHER LLP
* OPERATES AS
GREENBERG TRAURIG, S.C.
^ A BRANCH OF
GREENBERG TRAURIG, P.A.
FLORIDA USA
^ OPERATES AS
GREENBERG TRAURIG GRZESAK sp.k.
^ OPERATES AS
GREENBERG TRAURIG LLP
FOREIGN LEGAL CONSULTANT
OFFICE
** STRATEGIC ALLIANCE

legal memorandum prepared by PETILLION setting forth the specific legal bases and framework for the proposed model's compliance with GDPR attached as Annex A.

In sum, the proposal for a centrally managed registration data directory service (RDDS) by ICANN would alleviate or simplify various issues concerning GDPR principles and regulations. This model would establish a clearer distinction between the role of ICANN and the role of the contracted parties in the transfer, publication, access, and disclosure of domain name registration information and insulate the contracted parties from liability for such activities. Furthermore, ICANN has already done much of the work required to implement this model in compliance with GDPR. Notably, implementation of this model is not mutually exclusive to the work being done on the accreditation and access model as such, which would still be necessary regardless of whether ICANN is managing a centralized RDDS system or whether it is managed at the contracted party level.

In the proposed model ICANN would fully take the controller role with respect to the collection, access, and disclosure of personal domain registration information for WhoIs purposes, while the contracted parties would operate only as processors of such data on behalf of ICANN for WhoIs purposes. Under GDPR (Articles 28-34), liability of the processor is determined in relation to the GDPR obligations that must be laid down in the contractual framework. Liability is also separately determined for separate processing activities. Accordingly, if a clear distinction is made between the different processing activities in the RDDS processing chain in the contractual framework between ICANN and the contracted parties then the contracted parties, in their role as processor, would be responsible only for the collection and transfer to ICANN of thick WhoIs information. Once the information is transferred to ICANN and organized/managed by ICANN in a central repository, the processors (i.e., the contracted parties) must no longer be involved in any subsequent ICANN processing activities. As a result, any liability relating to, for example, the unreasonable disclosure of personal data contrary to art. 5 and 6(1)(f) GDPR or the violation of data subjects' rights contrary to articles 15-22 GDPR relating to access to and disclosure of centralized RDDS, data would be solely incurred by ICANN. The necessary contractual framework could be accomplished either by amending the existing agreements or through a new specification. Furthermore, ICANN has already identified the necessary requirements for this model to comply with the obligations of the GDPR in Appendix C of its Temporary Specification for gTLD Registration Data. In a centralized RDDS model, the data processing requirements for contracted parties specified in Appendix C would need to be implemented by ICANN as the controller of the data in a centralized RDDS model.

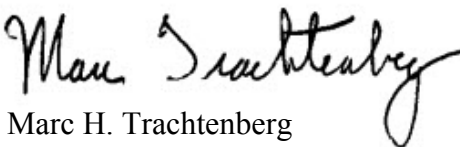
Contracted parties would of course still be controllers of some domain name-related personal data for other purposes. For example, data collected and processed in order for persons to enter into registration agreements with registrars and for registrars to process payment transactions for registration of domain names and ancillary services. However, even if some of the data elements collected and processed by the contacted parties for other purposes are the same as data elements collected on behalf of ICANN for WhoIs purposes, the processing activities are still separate from a GDPR perspective. For example, if the name, physical address, and email address of a registrar's customer collected to process the credit card transaction to pay for registration of a domain name is the same information listed for the registrant of that domain name, under GDPR these processes are still separate. So,

while the registrar may be the controller of that personal data for purposes of processing the credit card transaction, it is still only a processor for ICANN of the data with respect to its separate collection and transfer of the information to ICANN for WhoIs purposes.

Obviously, this model would require a significant amount of personal data to be transferred from the EU to ICANN in the United States. Transfers of personal data from the EU to another jurisdiction require either an adequate level of protection in the receiving jurisdiction or the provision of sufficient safeguards to guarantee compliance with the GDPR principles and the security of the data. Since the U.S. has not been found to provide an adequate level of protection, such safeguards would need to be implemented in the contractual framework. This can be done by utilizing the Model Clauses adopted by the EU Commission and/or putting in place an approved code of conduct between ICANN and the contracted parties.²

As discussed above, for more detailed and specific legal analysis, please review the attached memorandum. Please let me know if there is any other information that we can provide that would be helpful for the call. I look forward to speaking with you next week.

Best regards,



Marc H. Trachtenberg
IP/Tech Shareholder

Enclosures

Cc: John Jeffrey, General Counsel, Internet Corporation for Assigned Names and Numbers
Flip Petillion, PETILLION
Alexander Heirwegh, PETILLION
Jan Janssen, PETILLION

² ICANN could certify itself under the EU-US Privacy Shield. However a recent non-binding EU Resolution has called the Privacy Shield framework into question and has asked for the suspension of the Shield unless the U.S. complies with the GDPR principles by September 1, 2018.

ANNEX A

MEMORANDUM

CENTRALIZED RDDS FOR GTLD REGISTRATION DATA MANAGED BY ICANN - GDPR PERSPECTIVE

This memorandum intends to explore the practical and legal possibilities to implement a Registration Data Directory Service (RDDS) system for gTLD registration data that is centrally operated and managed by ICANN.

The current RDDS system, known as WHOIS, is operated in a decentralized way by numerous registrars and registry operators managing their respective databases. The anticipated adoption and implementation of the Registration Data Access Protocol (RDAP) would allow for the technical implementation of a centralized RDDS model incorporating differentiated access.

It does not expand on all technical, organizational and contractual measures necessary to practically implement this model, nor does it elaborate on all principles and requirements set out in the GDPR to achieve full compliance. The primary aim is to demonstrate the feasibility of the proposed model, specifically regarding certain key issues presented by the GDPR.

I. The proposed model: a centralized RDDS system for gTLD registration data managed by ICANN

In essence, the proposed model envisages a single, centrally-operated RDDS system for gTLD registration data that will function as follows:

As in the current WHOIS system, registrars will still be required to collect all (thick) RDDS data from the registrants. In contrast to the current WHOIS system, the RDDS data in the proposed model will not be maintained by registrars or registry operators in separate thin or thick RDDS databases but by ICANN in a central thick RDDS system.

The contracted parties will be required to transfer all collected registration data to ICANN, who will then aggregate and manage this data using RDAP in a centralized RDDS system. As a result, ICANN, and not the registrars or registry operators, will provide differentiated access to data on registered domains.

II. Regulatory and contractual framework

The operation of the RDDS system is maintained through a series of commitments under ICANN's agreements with the registry operators (Registry Agreements) and accredited registrars (Registrar Accreditation Agreement) and through several WHOIS consensus policies adopted by ICANN.

Recently, the WHOIS system in its original form was adapted to comply with increased requirements and obligations regarding the protection of personal data following the entry into force of the EU

This memorandum is provided for information purposes only and reserved for further discussion with ICANN and the IPC. It is not offered, nor should be construed, as legal advice.

PETILLION expressly disclaims all liability with respect to actions taken or not taken based on any or all of the information or other contents of this document.

General Data Protection Regulation 2016/679 (GDPR).¹ Both ICANN and EU authorities determined that an access model providing unlimited and undifferentiated access to all (personal) WHOIS data is not compatible with the principles and obligations under the GDPR.

To comply with the principles and obligations under the GDPR, ICANN adopted a Temporary Specification for gTLD registration data.² The Temporary Specification establishes temporary requirements with a view to having ICANN and its contracting parties comply with existing ICANN contractual requirements and community-developed policies in light of the GDPR, until a more permanent policy is implemented.

Most of the requirements determined in the Temporary Specification, especially those covered by its Appendix C, can also be applied to a model where ICANN performs a central role as the controller for the management and disclosure of registration data in a centralized RDDS system. There would thus be no need to replace the existing contractual framework between ICANN and the contracted parties. The RDDS-related provisions would only need to be amended to ensure the transfer of operational control to ICANN.

A GDPR-compliant RDDS system must be balanced with other regulatory frameworks and fundamental rights. In its fourth recital, the GDPR provides:

"The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."

The principle of proportionality requires that the measures taken to protect the privacy and data of natural persons are necessary and adopted in the least onerous way and balanced with the competing interests of the public and third parties. These rights include the freedom of and access to information, the right to an effective remedy, the right to conduct a business and the right to the protection of intellectual property. A centralized RDDS model should reflect such proportionality.

III. Comparable centralized registers

The operation and management of a centralized RDDS system is comparable to and serves a similar purpose as other EU public registers containing publicly accessible personal data, such as trademark registers and company registers. Both registers have been recognized as serving a public interest function, allowing the publication of relevant personal data in accordance with the principle of proportionality.

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), *OJ L. 119*, 4 May 2016.

² Temporary Specification for gTLD Registration Data, adopted on 17 May 2018 by ICANN Board Resolutions 2018.05.17.01 – 2018.05.17.09, available on <https://www.icann.org/en/system/files/files/gtld-registration-data-temp-spec-17may18-en.pdf>.

This memorandum is provided for information purposes only and reserved for further discussion with ICANN and the IPC. It is not offered, nor should be construed, as legal advice.

PETILLION expressly disclaims all liability with respect to actions taken or not taken based on any or all of the information or other contents of this document.

The EU and each of its member states operate a central trademark register containing, *inter alia*, the name and address of applicants and registered trademark holders.³ The EU Trademark Regulation expressly provides that “*all the data in the register, including personal data, shall be considered to be of public interest and may be accessed by any third party*”, and that, “*for reasons of legal certainty, the entries in the register shall be kept for an indefinite period of time*”.⁴ In light of the similarities between trademarks and domain names, especially regarding brand and consumer protection, and the important public interest function related to the transparency and accountability of domain name holders, there is no reason why such a consideration cannot equally pertain to information in a centralized international RDDS system.

Similarly, EU regulations require the collection, storage and disclosure of information, including personal information, regarding companies in a central national company register.⁵ The Court of Justice of the EU has specifically determined that the need to protect the public interest and the legitimate interests of third parties takes precedence over an individual's right to data protection when publishing a limited number of personal data items in such a public register.⁶

The adoption of a centralized RDDS model managed by ICANN would address one of the few differences that currently exist between trademark and company registers and the RDDS system, namely the fact that it is currently not managed and operated by a single responsible entity. Additionally, the centralized RDDS model would identify ICANN's operational role as the central manager of the RDDS system, comparable to the EU Intellectual Property Office for the European (trademark register and the specific government authorities for the national commercial registers. The identification of ICANN as controller by the ICANN community would allow ICANN to perform its processing activities in relation to a centralized RDDS model on the basis of Article 6.1(e) GDPR, which provides that “*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*”. A legal recognition of ICANN's authority (e.g., in an international agreement) would increase legal certainty, as it would not require the difficult balancing of the legitimate interests of ICANN and third parties against the privacy rights and interests of the data subjects.⁷

³ See Article 44, 111 and 112 of Regulation 2017/1001 Of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark, OJ L154 (EU Trademark Regulation).

⁴ Article 111.9 EU Trademark Regulation 2017/1001.

⁵ See Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law, OJ L 169, 30.6.2017, p. 46–127.

⁶ *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni (Manni)*, Court of Justice of the European Union (Second Chamber), 9 March 2017, C-398/15, ECLI:EU:C:2017:197.

⁷ This balancing exercise is currently required under Article 6.1(f) GDPR on which basis the different processing activities related to the RDDS system are performed in the absence of any recognition under the law. Article 6.1(f) provides that “*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.*”

This memorandum is provided for information purposes only and reserved for further discussion with ICANN and the IPC. It is not offered, nor should be construed, as legal advice.

PETILLION expressly disclaims all liability with respect to actions taken or not taken based on any or all of the information or other contents of this document.

IV. GDPR implications of the proposed model

A. General implications

The GDPR aims at providing data subjects with more insight in, and control over, the use of their personal data. The Regulation requires, *inter alia*, for all processing activities of personal data falling under its remit, that the data processing (i) is limited to what is necessary for specified legitimate purposes and stored for no longer than what is necessary for those purposes; (ii) is performed on the basis of a specific lawful ground; (iii) ensures the different rights of data subjects; (iv) implements the necessary contractual, technical and organizational measures to comply with the principles of the GDPR and to guarantee the security of the data; and (v) does not include the transfer to third countries without the provision of an adequate level of protection or appropriate safeguards.

A centralized RDDS model managed by ICANN would actually alleviate various issues with the above-mentioned GDPR principles and obligations. Primarily, the model would establish a clearer distinction between the role of ICANN and that of the contracted parties for the collection, transfer, storage, publication and disclosure of domain name registration data in the RDDS system.

A centralized model would amount to ICANN fully taking the role of controller in the framework of the centralized RDDS system, while the contracted parties only operate as processors. This does not mean that contracted parties will no longer be considered controllers in other instances. Apart from the RDDS system, contracted parties will evidently act as controllers for other processing activities in the context of the domain name registration chain. For example, registrars will still need to process the personal information of their customers for the performance of the domain name registration contract and to combat abuse. The distinction between ICANN as the controller and the contracted parties as the processors essentially implies that, in the context of RDDS, the contracted parties collect and transfer the (personal) information related to the registered domain names on the instruction and on behalf of ICANN, who determines the purposes and means of the processing. The contractual frameworks between ICANN and the contracted parties must thus clearly include binding instructions for the processing of the data, including with regard to transfers of personal data to the United States.

As the controller of the registration data in a centralized RDDS model, in order to comply with the principles and obligations of the GDPR, ICANN must:

- i. Observe the principles related to the processing of personal data laid down in Article 5 GDPR;
- ii. Identify its different processing activities, their related purposes and corresponding legal bases⁸;
- iii. Comply with the specific controller processing obligations, such as regarding the data subjects' rights, the maintaining of a record of processing, the implementation of security measures, the appointment of a data protection officer, etc.;⁹

⁸ As required under Article 5.1 (b), (c) and (e), and Article 6 GDPR.

⁹ See Articles 12-22 GDPR; Article 30 GDPR; Articles 32-34 GDPR; Articles 37-39 GDPR.

- iv. Establish a binding contractual framework supported by sufficient guarantees (e.g. an approved code of conduct or certification mechanism) to engage with the processors (i.e. contracted parties) in a GDPR-Compliant manner¹⁰; and
- v. Observe the conditions for transfer of personal information outside the EU to the US.¹¹

ICANN has already identified the general requirements necessary to comply with the obligations of the GDPR in Appendix C of its Temporary Specification for gTLD Registration Data.¹²

B. Differentiating between different data processing activities and purposes

A centralized RDDS model managed by ICANN would be construed as a differentiated access system, taking advantage of RDAP possibilities. Within that system, different data processing activities must be distinguished.

In accordance with the contractual instructions provided by ICANN, the accredited registrars would collect the full registration data from the registrants. Thereafter, the accredited registrars would transfer the full registration data to ICANN (either directly or via the relevant registry operator¹³). The transfer of the registration data would be conducted within the contractual processing framework between ICANN and the contracted parties.

The collection and transfer of this (personal) information is based, on the one hand, on the necessity for the registrar to perform the registration contract¹⁴ and, on the other hand, on the legitimate interest of the controller (ICANN) and third parties to establish and operate an effective RDDS system and to meet the legitimate needs of law enforcement, promoting consumer trust and safeguarding registrant data¹⁵.

ICANN will then aggregate the registration data it receives and differentiate between public information and non-public information. Public information must be made accessible to all users following a query in the centralized RDDS system. Non-public (personal) information should be disclosed only to authenticated third parties. Insofar personal information is to be considered as public information, the legal basis for disclosure would either be:

- the overriding legitimate interest of ICANN to disclose this information in relation to its identified purposes of *“addressing issues of competition, consumer protection, security, stability and resiliency, malicious abuse issues, sovereignty concerns and rights protection”*¹⁶; or
- the data subject’s consent to publicly disclose additional information¹⁷.

¹⁰ See Article 28 GDPR.

¹¹ See Articles 44-49 GDPR.

¹² See “Appendix C: Data Processing Requirements” of the Temporary Specification for gTLD Registration Data.

¹³ Comparable to what is already required through individual registry contracts under the current RDDS system.

¹⁴ In accordance with Article 6.1(b) GDPR.

¹⁵ In accordance with Article 6.1(f) GDPR.

¹⁶ ICANN Bylaws Section 4.6 (d); In accordance with Article 6.1(f) GDPR.

¹⁷ In accordance with Article 6.1(a) GDPR.

This memorandum is provided for information purposes only and reserved for further discussion with ICANN and the IPC. It is not offered, nor should be construed, as legal advice.

PETILLION expressly disclaims all liability with respect to actions taken or not taken based on any or all of the information or other contents of this document.

Subsequent access to, and use of, the information by third parties with a legitimate interest must be distinguished as having their own identified purposes (such as law enforcement, the investigation of fraud or consumer deception, or the enforcement of IP rights) and legal bases (legitimate interest).

Additionally, ICANN must ensure the reasonable disclosure of non-public registration data in response to a disclosure request based on an apparent overriding legitimate interest. A centralized RDDS access model would significantly reduce complexities related to authenticated and reasonable access to non-public registration data, as a single standardized access process can be established by ICANN in relation to all access requests.

C. Addressing concerns of the European Data Protection Board

A centralized RDDS model allows ICANN to put in place appropriate safeguards to ensure that (i) the disclosure is proportionate and limited to what is necessary, and (ii) the other requirements of the GDPR are met, including the provision of clear information to data subjects.¹⁸

Instead of ending up with diverging GDPR compliance measures by the contracted parties, ICANN can put in place a central and uniform data protection policy and code of conduct.¹⁹ A central code of conduct would, for example, enable ICANN to specify and manage appropriate retention periods for the data stored in the centralized RDDS system, in accordance with defined purposes and justifications (such as to establish or defend against future legal claims or to investigate crime or IP infringement).²⁰

Additionally, a central code of conduct may specify the necessary information that must be provided by the processors (registrars) to the data subject regarding the recording of their data in a centralized RDDS system that enables differentiated access to third parties. This information may include the fact that RDDS queries and access request to the registrant's non-public registration data will be logged and that they can possibly access these queries or requests in specific circumstances.²¹ Processors could also be required to inform the registrant that, upon the collection of the (personal) registration data, the registrant is free to (i) designate the same person as the registrant (or its representative) as the administrative or technical contact; or (ii) provide contact information which does not directly identify the administrative or technical contact person concerned.²² The latter option may also serve to justify differentiating between natural persons and legal entities for the disclosure of publicly accessible information in the centralized RDDS system. The unintended disclosure of personal information by a legal entity can be prevented by informing the legal entity registrant, at the collection of the information, that it has the option to provide non-identifiable contact information.

¹⁸ Letter of the European Data Protection Board to Mr. Göran Marby (ICANN), "1. Purpose specification and lawfulness of processing", EDPB-85-2018, 5 July 2018, 1-2.

¹⁹ Letter of the European Data Protection Board to Mr. Göran Marby (ICANN), "6. Codes of conduct and accreditation", EDPB-85-2018, 5 July 2018, 6.

²⁰ Letter of the European Data Protection Board to Mr. Göran Marby (ICANN), "5. Data Retention", EDPB-85-2018, 5 July 2018, 6.

²¹ Letter of the European Data Protection Board to Mr. Göran Marby (ICANN), "4. Logging of access to non-public WHOIS data", EDPB-85-2018, 5 July 2018, 5.

²² Letter of the European Data Protection Board to Mr. Göran Marby (ICANN), "2. Collection of "full WHOIS data"", EDPB-85-2018, 5 July 2018, 4.

This memorandum is provided for information purposes only and reserved for further discussion with ICANN and the IPC. It is not offered, nor should be construed, as legal advice.

PETILLION expressly disclaims all liability with respect to actions taken or not taken based on any or all of the information or other contents of this document.

In relation to their respective roles as processors in the centralized RDDS system, the contracted parties would need to comply with such a central code of conduct through the contractual processing framework.²³

D. Controller/processor contractual framework and the liability of contracted parties

A centralized RDDS model would require that a binding contractual framework is established between the controller (ICANN) and the processors (contracted parties) (*Cf.* Article 28 of the GDPR). Such a contractual framework could be established either by (i) amending the existing contractual frameworks between ICANN and the contracted parties (the Registrar Accreditation Agreements and Registry Agreements), or (ii) establishing a new contractual framework containing the instructions for processing and other GDPR-related obligations.

Either way, the contract between the controller and the processors must include, *inter alia*, (i) the obligation of the contracted parties to provide sufficient guarantees in relation to the principles of the GDPR; (ii) a clear delineation of the subject-matter, duration, nature and purposes of the processing; (iii) clear instructions for the processing by ICANN to the contracted parties; and (iv) the implementation of technical and organizational measures to adhere to the principles of the GDPR and to ensure the security of the personal data and to prevent data breaches.²⁴ This contractual framework may be supported by a central code of conduct and standard contractual clauses determined by the EU Commission or relevant supervisory authority.²⁵

The liability of the contracted parties (processor liability) is determined in relation to the obligations laid down in the contractual framework, in accordance with Articles 28 to 34 GDPR. To determine the liable party, a clear distinction must be made between the different processing activities in the chain of processing activities in a centralized RDDS.²⁶ The processors (contracted parties), in the framework of the processing contract, are responsible for the collection and transfer to ICANN of the full registration data. If, during these processing activities, a processor, for example, acts against the instructions of the controller (ICANN) or fails to implement sufficient organizational or technical measures to protect the personal data, it will be liable for violating its obligations under the GDPR.²⁷

However, once the information is transferred to the controller (ICANN) and organized in a central RDDS system, the processors are no longer involved in the subsequent processing activities. Liability relating to, for example, the unreasonable disclosure of personal data contrary to Article art. 5 and 6(1)(f) GDPR or the violation of data subjects' rights contrary to Articles 15-22 GDPR would then be solely incurred by the controller. Once ICANN has received the data from the contracted parties, it engages in new processing activities, separate from the controller/processor framework.

²³ Article 28.5 GDPR.

²⁴ Article 28.3 GDPR.

²⁵ Articles 28.7 and 28.8 GDPR. In this respect, please refer to Section IV. C. Addressing concerns of the European Data Protection Board, 6.

²⁶ In this respect, please refer to Section IV. B. Differentiating between different data processing activities and purposes, 5.

²⁷ Articles 28.1 and 28.3(a) and 28.10 GDPR.

E. Transfers

Another consequence of a centralized RDDS model is that, in many instances, the full registration data must be transferred outside the European Economic Area to the controller (ICANN) located in the United States. Such transfers require either an adequate level of protection in the receiving jurisdiction or the provision of sufficient safeguards to guarantee the compliance with the GDPR principles and the security of the data.²⁸ As the US has not been found to provide an adequate level of protection, such safeguards will need to be implemented in the controller/processor contractual framework.

Appropriate safeguards can be implemented by adopting standard data protection clauses adopted by the EU Commission and/or by putting in place an approved code of conduct between ICANN and the contracted parties guaranteeing the compliance with the principles and obligations of the GDPR after the transfer. ICANN also has the possibility to certify itself under the EU-US privacy shield framework. However, a recent non-binding EU Resolution has called the Privacy Shield framework into question and has asked for the suspension of the Shield unless the US complies with the principles of the GDPR by September 1, 2018. As a result of the legal uncertainty surrounding the EU-US Privacy Shield, the preferred option would be to implement a specific contractual framework to ensure compliance with the requirements for transfer. That can be achieved by using standard contractual clauses and/or an approved code of conduct.

V. Conclusion

The adoption of a centralized RDDS model managed by ICANN would alleviate many practical and legal concerns related to the management and disclosure of registration data. A centralized model would allow ICANN to align its current supervisory role with a practical role as the manager of the central RDDS system. The model would mitigate a differentiated approach towards the collection and transfer of, access to, and disclosure of, registration data. It would increase legal certainty for third parties with an important legitimate interest to obtain and use registration information.

From the perspective of ensuring compliance with the GDPR, a central RDDS model would distinguish the roles of ICANN and the contracted parties more clearly. ICANN can be clearly identified as the controller and the contracted parties as the processors of the registration data. The model would facilitate compliance with the principles and obligations of the GDPR through the establishment of a uniform contractual framework for processing and of a central code of conduct.

²⁸ Articles 44-46 GDPR.