Wilson Sonsini Goodrich & Rosati, LLP
Avocats - Advocaten - Rechtsanwälte

Rue Montoyer 47
1000 Brussels
Belgium
PHONE +32 2 274 57 00
FAX +32 2 274 57 99
www.wsgr.com

# M E M O R A N D U M

**To:** Internet Corporation for Assigned Names and Numbers

**From:** Christopher Kuner and Bastiaan Suurmond

**Date:** September 25, 2017

**Re:** **Final responses to EU data protection questions re gTLD Registration Directory data**

## I. Background

The ICANN Generic Names Supporting Organization ("**GNSO"**) Next Generation gTLD Registration Directory Services ("**RDS**") Policy Development Process ("**PDP**") Working Group ("**WG**")'s charter includes "analysing the purpose of collecting, maintaining and providing access to gTLD registration data (…) and safeguards to protect that data." On that basis, the WG is tasked to "determine if and why a next-generation Registration Directory Service is needed to replace WHOIS (…)" – that is, the current system which provides public access to registration data collected when a domain name is registered. In addition, the WG is tasked with "creating policies and coexistence and implementation guidance to meet those needs."

The WG seeks to enhance understanding of key data protection frameworks and to inform the WG's deliberations about the application of data protection laws to gTLD registration data and directory services policies. To this end, the WG has requested Wilson Sonsini Goodrich & Rosati (WSGR) to provide an independent legal assessment of questions developed by the WG. The questions have been drafted by members of the WG for consideration by the panel of Data Commissioners who participated in the ICANN58 meeting in Copenhagen. We understand that the WG intends to make the final version of this memorandum freely available.

## II. Scope

This memorandum provides an independent legal assessment of questions developed by the WG, based on legal analysis of key data protection and privacy laws of the European Union

("**EU**") that may potentially apply to gTLD registration data and directory services, including especially (but not limited to) the EU Data Protection Directive 95/46/EC (the "**Directive**" or **"Data Protection Directive"**) and the EU General Data Protection Regulation 2016/679 (the "**GDPR**"). This memorandum focuses solely on legal issues, and will deal with legal requirements at the European level only. It focuses mainly on EU law, but also deals with other related areas of European law (e.g., the European Convention on Human Rights). This memorandum does not address national law. It incorporates our responses both to the questions listed herein and to the supplementary questions that we have received from the RDS Leadership Team. Our responses focus solely on the questions asked, and are to be understood in that context. Our answers sometimes go beyond gTLD registration data when this is relevant to answering the respective question.

The GDPR will come into force on 25 May 2018, and given that the Directive will then no longer be in force, we have focused mainly on the GDPR in our responses.

## III. Answers to the WG's questions

### Purpose

1. *Our working group is now deliberating upon the purpose of domain name registration data and the registration directory system that provides public access to that data. Can you please help us understand what the data protection supervisors have meant over the years when they have told ICANN to specify the purpose of WHOIS? How would you assess the purpose of collecting, processing, maintaining and providing access to gTLD registration data? For example, can you help us understand what a purpose applies to when it comes to registration data or directory services? Where will purpose be applied (and not be applied) in registration data and directory services policies? What criteria should be used to determine legitimate purpose(s)? What is the difference between "primary" and "secondary" purposes and how does that affect all of the above?*

Under EU data protection law, personal data may only be collected and processed for specified purposes. The entity that decides the means and the purposes of processing is the data controller. Prior to collecting any personal data, the data controller must decide on the purposes for which it needs the data. This is a prerequisite for compliance with the other principles, such as data quality, data minimization, and transparency. Enumerating the purposes allows the data controller to assess, among other things, what data is required to achieve the purpose, for how long it must be retained, and to whom the data may be disclosed.

There is no precise legal definition of the distinction between primary and secondary purposes. Primary purposes are the main purposes for which the data are processed, but the difference between the two depends on the circumstances in each particular case. Each purpose requires its own legal basis for processing.

The purpose limitation principle also enables the data controller to comply with the transparency principle, which requires individuals to be provided with adequate information

so that they may understand the extent to which their data are being processed. If the data controller has not properly articulated the purposes, it is not able to communicate to the individual what exactly it intends to do with the data. Additionally, if processing is based on the consent of the individual, the individual must be "informed" for their consent to be valid (as discussed in greater detail under Question 2 below).

As the Article 29 Working Party (the body of EU data protection regulators) explains: "the principle of purpose limitation is designed to establish the boundaries within which personal data collected for a given purpose may be processed and may be put to further use" (Article 29 Working Party, Opinion 03/2013 on purpose limitation (WP203), p. 4). To effectively establish those boundaries, the purposes must be specific and explicit, but there are no hard and fast rules as to the level of detail with which the purposes must be described. To prevent lengthy "legalistic" notices that are hard to understand, the Article 29 Working Party recommends a "layered" approach, in which the purposes are summarized concisely, with a link to a more detailed breakdown of the purposes.

Defining the exact purposes for the processing of WHOIS data is outside the scope of this memorandum. However, we have the following general suggestions: (1) consider the reasons for which the databases exist, and proceed from that; (2) do not include too many purposes, i.e., focus on the main ones; (3) and use clear and non-legal language that can be understood by ordinary individuals as much as possible. Clearly defining and limiting the purposes of processing is important to comply with the purpose limitation principle, which is essential to provide a valid legal basis for data processing.

Without being able to specify the exact purposes here, we generally believe that the primary purposes of registration data and directory services would relate to the actual registration of domains and the functioning of the domain name system. Purposes that go beyond this (e.g., collecting data to combat IP violations) would be considered to be secondary purposes. An example of a generic purpose could be the following: "Personal data are processed in order to allow individuals and organizations to register, manage, and transfer Internet domain names".

Once the data controller has defined a purpose, it can determine what personal data and what processing would be necessary to achieve that purpose. Personal data must be adequate, relevant, and limited to what is necessary to achieve the purpose. For example, if a purpose is defined as "allowing individuals and organizations to register, manage, and transfer Internet domain names," then it may follow that ICANN must retain certain information to contact and authenticate the registrant, but it may not follow that ICANN must share this information or make it public. The latter processing activities would arguably serve a different purpose, which should be defined separately and have their own legal basis.

In view of the principle of privacy by design, we recommend that ICANN conduct a formal process to define the primary and secondary purposes, the necessary data and processing activities, as well as the appropriate legal bases. Because of the scale of these processing activities, we also recommend conducting a Data Protection Impact Assessment ("**DPIA**"). A useful guide to conducting a DPIA has been published by the UK Information Commissioner's Office.

2. *Article 6(1)(b) Directive provides that personal data may only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (Article 7). Processing of personal data is allowed to a limited number of legitimate grounds, specified in Article 7 Directive. Under what circumstances might the publication of registration data elements that are personal data be allowable?*

This question requires consideration of two of the major issues in assessing the legality of registration databases, namely purpose limitation and having a ground for data processing. Purpose limitation has been addressed in detail in our response to Question 1.

With regard to legal bases (grounds) for data processing, this is addressed in Article 7 Directive and Article 6 GDPR. These grounds can include the individual's consent, necessity to perform a contract, compliance with a legal obligation, and the data controller's legitimate interest, among others.

The two main legal bases mentioned in Article 7 Directive that are relevant here are the consent of the individual whose data are being processed, and the legitimate interest of the data controller unless this is overridden by the fundamental rights and freedoms of the individual. We discuss each of these legal bases in more detail later on in this memorandum. Other legal bases set out in Article 6(1) GDPR are not discussed here because they are of limited application to the domain registration context (i.e., processing that is necessary for the performance of a contract; compliance with a legal obligation; protection of the vital interests of the data subject; and performance of a task carried out in the public interest), though some of them are discussed in our responses to later questions.

As explained in the response to Question 15, the conditions for application of the "legitimate interest" grounds are restrictive and uncertain, and would be unlikely to be applicable to all the possible uses to which registration data could be put. Generally speaking, we think that consent is the more stable legal basis that could potentially be used for the processing of registration data by data controllers, though it would have to be implemented carefully and would impose a number of strict conditions; the use of consent is further described in the response to Question 11.

**Registration Data Elements**

3. *Considering that gTLD registration data elements may refer to mere technical information, information that may relate to legal persons and information that may directly relate to an identified or identifiable natural person, only the last one of which has consequences from a data protection perspective, how do you think <u>consistent policies</u> for a Registration Directory Service could best be developed?*

   *For example, it is our understanding that "personal data" under the EU Data Protection Directive and the General Data Protection Regulation is specified if data relates to an identified or identifiable natural person. Currently, Registrars and Registries display the following info through a public directory service called WHOIS without any access restrictions: the domain name registrant's full name, street*

*address, zip code, country code, telephone number and email address. Is this "personal data" as specified by the Directive and the General Data Protection Regulation, regardless of whether the registrant is a legal person or a natural person?*

In order to answer this question, it is necessary first to review the relevant legal issues with regard to the definition of personal data.

Data elements are considered to be personal data if they relate to an identified or identifiable natural person (i.e., an individual). This depends on the context and the particular data element involved, and data that may not seem identifiable on their face may still be considered to be personal data (e.g., a 16-digit number may actually be a credit card number). Given the growth of computing power, much data that was earlier not considered to be personal has become viewed as personal data, so the concept is fluid. Under current data protection law (i.e., the Directive and national implementations of it), the data of legal persons is covered in only a few jurisdictions, while under the GDPR, it will not be covered by data protection law at all (see Recital 14). The GDPR gives as example of the data of legal persons, their name and form as well as their contact details, which it states, are not covered. However, the key factor is not just whether the name of the registrant is that of a natural or legal person, but how the different data fields, when taken together, relate to an individual.

Data in the WHOIS directory would not be covered by data protection law if it relates purely to a legal person. However, it should be noted that there are many situations where it can be difficult to separate the data of natural persons from that of legal persons. This can be the case, for example, if the legal person is a sole proprietorship, if the name of a person appears in the company's name, if the business address is a natural person's residence, or if an email address is assigned to a single individual (john.doe@company.example.com as opposed to info@company.example.com). The tendency to consider much company-related data as having an impact on the data protection rights of individuals can be seen in judgments of the Court of Justice of the EU (the "**CJEU**") (e.g., the *Bavarian Lager* case, Case C-28/08 P, concerning the names of participants in a business meeting; and the *Bara* case, Case C-201/14, concerning the processing of tax data of an individual by a public administrative body). Thus, it could be difficult in practice for ICANN to implement a policy that clearly separates the data of legal entities from personal data.

With regard to consistent policies, it may be impossible to completely eliminate the processing of personal data (i.e. data of individuals) in the databases. However, ICANN could try to strive to implement data minimization principles, such as by limiting the amount of clearly personal data when a domain is registered. We note that the current section 1.4.2 of the 2013 Registrar Accreditation Agreement ("**RAA**") includes a considerable amount of data, some of which could potentially be considered to be personal data if it is considered as a whole (e.g., e-mail addresses, contact telephone numbers, etc.). Section 1.4.2 also states that "additional data elements can be added", which opens the door to the inclusion of additional types of data (we refer here also to our response to Question 5).

We believe that ICANN should review the amount of data collected and try to limit it to what is strictly necessary, and also try to limit the ability of other parties to include other types of

data that are not listed. This could include requiring that contact points be listed solely as functions (e.g., "Tech Department"), in which case they would likely not be considered to be personal data. The possibility to include free text should also be limited. This sort of data minimization would help limit the data protection risks.

4. *Article 5 of the EU commerce directive requires service providers to disclose their contact information. Does this directive apply to domain name registrants? Does that mean that registrants that are service providers in the EU could be required to have their contact data displayed in a registration directory service?*

We believe that it is likely that Article 5 of the e-Commerce Directive 2000/31/EC (the "**e-Commerce Directive**") would be found to include domain name registration services, but that this coverage would not always extend to registrants. Even if some registrants are covered, this does not necessarily mean that their contact data could be freely used for other purposes.

The e-Commerce Directive creates the basic legal framework for online services, including electronic commerce, in the EU Internal Market. Article 5 applies to providers of "information society services", such as web shops and other online service providers. Under Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC, information society services are those that are normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services (note that Directive 98/34/EC was repealed and replaced in 2015 by Directive (EU) 2015/1535, which however contains the same definition of information society services in Article 1(1)(b)). With regard to providing services for remuneration, the controlling factor is not whether remuneration is actually requested, but whether the services at issue are normally provided for remuneration.

Providing domain name registration services seems to meet these criteria, since these services are normally provided for remuneration, at a distance, by electronic means, and at the individual request of the registrant. With regard to registrants, it seems that some, but not all, may fall within this definition. Thus, many registrants may not provide information society services via the domains they register (e.g., they may not establish functioning web sites, or their web sites may provide information without requesting remuneration), in which case the definition would not apply to them.

Even if registrants are found to provide information society services, Article 5 e-Commerce Directive could still not be used as a legal basis for large-scale use of all data in the WHOIS database. Article 5 requires publication of a limited amount of data for the purpose of allowing the identification of service providers, and it seems that the data contained in WHOIS may go beyond this. It also does not allow use of the data for purposes beyond providing information and transparency for users. Finally, data disclosed under Article 5 is still subject to the data protection requirements discussed throughout this memorandum (such as purpose limitation, proportionality, and others), and processing of any such data would be subject to restrictions under them.

If legal persons were allowed to self-identify as legal persons, this would not change the data controller's obligations with regard to protecting personal data *per se*. The imposition of

duties under data protection law is controlled by how data are actually processed, not by how parties choose to characterize data processing. However, if self-identification creates a process by means of which less personal data is included in the registration (e.g., by including only the data of legal persons, which is not considered to be personal data), then it may lower the legal risk.

Facilitation of compliance with Article 5 of the e-Commerce Directive would not itself provide a legal basis for disclosing data in registration directory services, since "facilitation of compliance" is not a recognized legal basis for data processing in data protection law.

5. *Below is an example of "thin data" elements made publicly accessible in today's WHOIS system for every registered gTLD domain name. Do you believe that any of the following data elements are considered personal information under the General Data Protection Directive, and why?*

> *Domain Name: CNN.COM*
> *Registrar: CSC CORPORATE DOMAINS, INC.*
> *Sponsoring Registrar IANA ID: 299*
> *Whois Server: whois.corporatedomains.com*
> *Referral URL: http://www.cscglobal.com/global/web/csc/digital-brand-services.html*
> *Name Server: NS-1086.AWSDNS-07.ORG*
> *Name Server: NS-1630.AWSDNS-11.CO.UK*
> *Status: clientTransferProhibited*
> *https://icann.org/epp#clientTransferProhibited*
> *Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited*
> *Status: serverTransferProhibited*
> *https://icann.org/epp#serverTransferProhibited*
> *Status: serverUpdateProhibited*
> *https://icann.org/epp#serverUpdateProhibited*
> *Updated Date: 15-feb-2017*
> *Creation Date: 22-sep-1993*
> *Expiration Date: 21-sep-2018*

In responding to this question, we note first that, as indicated by the RDS Leadership Team, we should also focus on all the WHOIS data contained in section 1.4.2 of the 2013 RAA.

As we have mentioned earlier, information is considered to be personal data if it can be related to an identified or identifiable natural person. In looking at the data in the "thin data" list in the question and in section 1.4.2, we can divide them into three categories:

(1) Some data types are clearly personal data because they identify a natural person directly (e.g., the name of a human being).

(2) Some data types do not fall under this definition because they refer only to legal persons rather than natural persons (e.g., the names of companies, unless it is a company where the family name or a personal name is used).

(3) Some data types do not seem on their face to identify an individual (e.g., the date a domain was created, or the name of a server), but may create a relationship to an individual nevertheless.

The concept of "identifiable" data is flexible and depends on the context in which the data is used. To give an example, saying that a person is "a lawyer in Brussels" does not make them identifiable. Saying then "a lawyer in Brussels who has an office in the centre of town" makes them more identifiable. And adding then that they are "a lawyer in Brussels who has an office in the centre of town and drives a Mercedes" would make them more identifiable still. Thus, identifiability depends on the context, and information that by itself is not identifiable may become so when considered together with other information. The CJEU has defined the standard for identifiability in its judgment in *Breyer*, Case C-582/14 dealing with whether IP addresses are personal data, where the Court stated that data are not identifiable "if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant" (para. 46).

It can be seen that the information in category (1) above will always be personal data, while the data in category (2) will (almost) never be personal data. The problem is category (3), which concerns the majority of data. For this category, identifiability will usually depend on the context in which it is used, and the possibility of combining it with other data sets. Because, as explained throughout this memorandum, scrutiny of limitations on data protection rights or potential infringements of them is strict, European courts and regulators often tend to find that such data is identifiable, unless there is an ironclad case for believing that it is not. That is, as a general conclusion, they tend to adopt a default position that even information that on its face might not seem identifiable could actually be so, because the consequence of finding it not to be identifiable is to remove processing of the data from the scope of data protection law, thus putting the fundamental rights of individuals at risk. This conclusion is also compelled by the high value that the CJEU has given to the right to the protection of personal data.

Thus, with regard to the registration data contained in category (3), the answer is "it depends". The contextual nature of the definition of personal data means that even data fields such as registration date, expiration date, updated date, and registrar name could potentially be found to constitute personal date, if taken together or in combination with other data they could serve to identify an individual. The fact that certain text fields may be added by a registry or registrar but are not required by ICANN could change a finding of who the data controller is, but would not change their characterization as personal data (or not). The determining factor is the data that are entered in the field, not the definition of the field. We believe that it is safer for ICANN to assume that most of this data could be found by a court or regulator to be personal data. This is also true because it is stated in section 1.4.2 that additional text fields can be added, so that the scope of the data may be beyond what is listed.

It is important to add that the fact that the data would be viewed as identifiable and thus as personal data does not necessarily mean that it could not be processed in a specific situation, just that it would likely be found to fall under data protection law. We believe that accepting

this situation and working within the rules of data protection law would be more in ICANN's interests than trying to argue that specific data fields do not constitute personal data.

**Access to Registration Data for Criminal and Abuse Investigations**

6. *It is our understanding that the suppression of criminal offences is an exemption to the application of the General Data Protection Regulation. If or when could this exemption apply to private cybersecurity firms investigating crime, civil offenses, or abuses in general by using data obtained through a registration data directory service?*

There are two provisions of the GDPR that could be referred to here. First, under Article 2(2)(d), 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, including the safeguarding against and the prevention of threats to public security" falls outside the scope of the GDPR. Under Directive (EU) 2016/680 (the so-called "Police Directive"), "competent authorities" are defined as "not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive" (Recital 11). If Member State legislation grants police-like powers to private cybersecurity firms, then it is possible that their activities would be seen to fall outside the GDPR, though they would still be subject to the Police Directive and other applicable EU law (such as human rights law). However, we are unaware of any such legislation in a Member State.

Second, under Article 23(1)(d) GDPR, the scope of some of the obligations and rights in it may be restricted by EU law or Member State law when this is necessary to safeguard "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…" However, it seems unlikely that this would apply to the activities of private cybersecurity firms, for the following reasons:

(1) Such restrictions would have to be provided in EU or Member State law (most likely legislation), and we are not aware of any such legislation at the EU or Member State level.

(2) In the EU the prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties is exclusively reserved to public law enforcement authorities, such as the police. At the very least, any exception to this would require specific legislation at the EU or Member State level. The possibility of such specific legislation granting exceptions to data protection legislation for cybersecurity firms was recognized by the CJEU in 2013 in *Institut professionnel des agents immobiliers (IPI),* Case C-473/12, where the Court held that Belgian legislation regarding the activities of estate agents allowed their use of private detectives to fall within Article 13(1)(d) of the Data Protection Directive (which contains the possibility to provide exceptions to data protection rules similar to Article 23 GDPR). However, the Court found that such exceptions are not mandatory, but that they "may" be provided by Member States (para 48). Again, we are unaware of any such

legislation in either EU or Member State law that grants quasi-police powers to private cybersecurity firms.

It should also be pointed out that, even were such any restriction of data protection rights under Article 23 GDPR to apply, its application would be limited. First of all, Article 23 does not remove the application of data protection law, it just restricts the exercise of certain rights. Second, Article 23(1) provides that any such restriction must respect "the essence of the fundamental rights" and constitute a "necessary and proportionate measure in a democratic society". Thus, any restriction of data protection rights in favor of private cybersecurity companies would be strictly construed, and would still be subject to limitations under EU fundamental rights law.

7. *If the application of General Data Protection Regulation provisions led to a completely private domain name registration database, where the vast majority of registrants refused to give access to their data, should the economic repercussions of closing the database be taken into account, to evaluate whether or not to apply the General Data Protection Regulation? For example, would economic repercussions be seen as threatening the 'monetary interests of the State' or the economic rights of private cybersecurity firms and the IP industry?*

We understand that the reference to a "completely private domain name registration database" is intended to refer to a database with access restricted. We would point out that application of the GDPR is not affected by the fact that a database is privately run or that the data in the database are not accessible to the general public.

With regard to the second part of the question (whether the economic repercussions of closing the database would be taken into account), the question seems to refer to Article 23(1)(e) GDPR, which allows EU or Member State law to restrict certain rights and obligations under the GDPR when this is necessary to safeguard "other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security". The same considerations we set out above in responding to Question 6 would also apply here. That is, there would have to be restrictions of rights enacted in EU or Member State law; such restrictions would be strictly construed; and EU fundamental rights law would still apply.

The general thrust of the question seems to concern the place that the economic repercussions of restricting access to the domain name system would have in data protection law and EU law. In this regard, the CJEU ruled in several judgments on the balance between data protection rights and Internet-related economic rights such as the protection of IP (e.g., *Promusicae*, Case C-275/06; *LSG*, Case C-557/07; *Scarlet*, Case C-70/10; and *Bonnier*, Case C-461/10), and held that such balance must be determined under the EU legal framework for fundamental rights. It has not granted absolute protection either to data protection rights or to related economic rights that may be in conflict with data protection. However, we also note that the CJEU has ruled in *Google Spain*, Case C-131/12 that serious interference with an individual's data protection rights cannot be justified by the economic interest of a search engine operator (para. 81), and that in *Schecke*, Joined Cases C-92/09 and C-93/09 it found

that economic interests cannot be given automatic priority over data protection rights (para. 85). This means that any economic repercussions such as are mentioned in the question would be judged within this framework.

Thus, the economic repercussions of a measure are relevant, but they cannot by themselves justify a restriction of a fundamental right such as data protection. Given that in July 2017 the CJEU has re-emphasized that any limitations on the right to data protection should apply only as strictly necessary (*Opinion 1/15*, para. 140), and in light of the Court's statements in the *Google Spain* and *Schecke* judgments referred to above, we believe that it is highly unlikely that the economic effects of data protection law would have any influence on the CJEU, since the Court balances rights, and "economic repercussions" are not rights.

**Personal Privacy/Human Rights**

8. *Today, a public access WHOIS directory service enables anyone who may be the victim of defamation, threats, harassment, etc., to look up the name of a domain name registrant (which may or may not correspond to the owner of a website hosted at that domain name), as a deterrent to such attacks. Do you believe this deterrent effect can constitute a public service, instead of protecting the privacy rights of the perpetrators? This effectively contributes to the fight against online violence against women, who are often the victims in such cases.*

There are two issues to be distinguished here, namely (1) the purpose of the processing of personal data, and (2) the general extent and scope of processing. The GDPR requires that personal data be processed for a legitimate purpose (Article 6(1)(b)), but EU fundamental rights law also requires that data processing be proportionate (see *Digital Rights Ireland*, Joined Cases C-293/12 and C-594/12, para. 45). There is no doubt that combating defamation, threats, and harassment is a legitimate purpose. However, the database can also be used for many other purposes that may not be legitimate. Therefore, it would be necessary to limit use of the database to some defined purposes that are legitimate. Furthermore, under data protection law there are limits to the processing of personal data even if it serves a legitimate purpose.

The second issue is how the data are accessed in order to carry out the purposes for which they are processed. Questions arise in this regard, for example, as to whether unlimited public access to the data of every registrant complies with the requirement that data are "limited to what is necessary in relation to the purposes for which they are processed ("data minimization")" (Article 6(1)(c) GDPR). This ultimately involves the question of whether data processing using the database is excessive in scope or access (i.e., whether it violates the principle of proportionality), for example with regard to the accessibility to the general public of a large number of data fields.

Such a proportionality analysis includes consideration of the question of whether other, less intrusive means cannot be used to reach the desired result. As discussed in this memorandum, we believe there are a number of steps that could be taken to deal with many of the data protection issues (e.g., layered access, etc.), and that these could lessen the risk that the

widespread availability of the database could be found to be disproportionate. Without taking these steps, we do not believe that the appeal to purposes such as fighting defamation etc. would be enough by itself to justify widespread public access.

9. *Under the General Data Protection Regulation, is consumer protection an objective pursued by the State which would fall into the category of protecting the rights and freedoms of others? If yes, do you consider anonymous public access to registration data an additional protection given to consumers, to help them avoid scams?*

Consumer protection is not mentioned explicitly in the GDPR, though it is indeed a policy pursued by the State, and is even mentioned in the EU Charter of Fundamental Rights (Article 38, stating "Union policies shall ensure a high level of consumer protection"). However, the fact that anonymous public access to registration data may have some potential beneficial use with regard to consumer protection cannot by itself override the fundamental right to data protection. An example can be seen in the CJEU's *Google Spain* judgment, where the Court considered the legality of a search engine that could result in access to a "structured overview of the information relating to" an individual (para. 80). Although it recognized that other rights and interests were at stake (including economic interests), the Court found that a "fair balance" between them should be struck in favor of data protection rights (para. 81). We also refer again to para. 85 of the CJEU's *Schecke* judgment, where the Court found that the legitimate objective of transparency did not have automatic priority over the right to data protection.

We thus believe that, in light of the large amount of personal data contained in the database, the fact that it is publicly accessible, and the possibility that third parties could use it for a multitude of undefined purposes, the CJEU would regard any benefit to consumer protection as subordinate to the right to data protection.

10. *With regards to General Data Protection Regulation compliance by entities within the EU, would it be enough legally if ICANN consensus policies define a new Registration Directory Service which allows for controlled access to registration data, without requesting the data subject's formal consent for each use, especially uses that do not benefit him/her, but are lawful (for example, the suppression of criminal offenses)?*

We understand that "controlled access to registration data" means that access to the database would be limited, such as by ICANN approving accounts before they were able to access it. Taking this step would help ameliorate some of the data protection concerns about the database, but not all of them.

Some of the concerns about the WHOIS database have related to the extent and amount of data made publicly available, and the purposes to which it is subsequently used. Restricting access to the database to approved users would mean data would be used by fewer users for fewer purposes. Indeed, the letter from former Article 29 Working Party Chairman Peter Schaar on 22 June 2006 makes it clear that some form of layered access to the database could be useful in addressing data protection concerns. Although this is different from the approach suggested in the question above, it would also involve some form of restricted access.

In a layered system, the public directory could still include all non-personal data of corporate registrants. But for registrants who are natural persons, the public directory would only include registrant's email address, or even a "masked" email address (i.e. an email address operated by a third party, such as the registry or registrant that automatically forwards the message to the registrant's personal email address, without disclosing the email address to the sender), and the contact information of the registrar.

That way anyone seeking to contact the registrant can do so, without the registrant being exposed. If the registrant is unresponsive, the sender could seek disclosure of the registrant's contact information by submitting a request to the registry or registrant. The disclosure policy would dictate how such requests are handled. At a minimum, this policy could require the requestor to motivate his or her request, and require some form of identification. At its most protective, the policy could require the requestor to show a warrant or court order before disclosing the registrant's information.

The disclosure policy should be carefully crafted to balance the relevant rights and interests. We would recommend performing a Data Protection Impact Assessment ("**DPIA**"), to decide what data should be disclosed, to whom, and under what conditions.

Restriction of access would reduce the number of users of the data, and could thus lower the risk level. However, it would not solve per se the issues relating to use of the data. In order to deal with these issues, those given access to the data would also have to be obligated to restrict their use of it, such as when they sign up for access to the database, and such restriction would have to be enforced.

11. *Numerous stakeholders at ICANN have suggested that asking end users or beneficial registrants to consent to further uses of their registration data would solve the debate over the privacy of registration data made accessible through WHOIS. What are your views on the use of consent in this context?*

We believe that consent could help deal with some of the data protection issues faced with regard to the WHOIS database, but that it would also present challenges.

Consent is restrictively defined in EU data protection law, as is indicated in the GDPR. Under Article 4(11), consent must be freely given, specific, informed, and unambiguous. In the context of the WHOIS database, this would mean that consent would have to (1) be implemented in a granular fashion; (2) clearly set out the purposes of data processing; (3) provide the individual with information about how their data will be processed before the data are collected; (4) be expressed in a clear and unambiguous fashion; and (5) be revocable.

Note that the GDPR's requirements will apply to all data processing that takes place as of its entry into force. This means that, if personal data have been collected before that date, their subsequent processing will still be subject to the GDPR. The consequences of this position are mitigated somewhat by the fact that most of the conditions for consent were already reflected in EU data protection law, i.e., in many areas, the GDPR codified requirements that already existed.

We think that the requirements for valid consent have the following implications:

(1) Any consent should be implemented in a granular fashion. This means that, for example, consent for further uses of registration data should be separate from any consent for registration of a domain name (i.e., individuals should be able to consent to register domains without being forced to consent to further use of their data as well).

(2) The purposes of data processing would have to be set out specifically (this issue is discussed in more detail in Question 1). We think that the list of purposes should be limited.

(3) Clear information would have to be provided to individuals about the implications of their consent, and would have to be clearly phrased.

(4) Procedures would have to be put in place to deal with cases when individuals wanted to withdraw or revoke their consent. The withdrawal of consent does not affect the legality of data processing prior to withdrawal. The GDPR does not address the consequences of withdrawal of consent, and withdrawal must be possible at any time.

From the above, it can be seen that asking for consent would not be simple, would not solve all data protection issues, and would pose a number of organizational challenges.

**Jurisdiction**

12. *Can you explain to us how the data commissioners factor in the European Charter of Rights (or, for that matter, local or supra-national fundamental rights instruments in the case of countries outside Europe) in the assessment of data protection issues? Is this matter within their jurisdiction?*

There is not a single "European Charter of Rights". Rather there are two instruments that the question may be referring to, namely the Charter of Fundamental Rights of the EU, and the European Convention on Human Rights. The relationship between the two is complex, but we will explain it briefly here, and will also explain why the DPAs take both into account in their assessment of data protection issues.

The Charter of Fundamental Rights (the "Charter") is an instrument of EU law that sets forth the fundamental or human rights that exist under EU law and how they apply. It has the rank of primary or constitutional law, and thus overrides any conflicting rules. The CJEU is the highest level court that interprets the Charter.

The Convention on Human Rights (the "Convention") is an international treaty that was adopted by the Council of Europe, a human rights organization headquartered in Strasbourg of which all EU Member States (and 19 other countries) have joined. The highest level court interpreting the Convention is the European Court of Human Rights.

As the Council of Europe is not an EU entity, the Convention is not an instrument of EU law. However, there are close ties between the Charter and the Convention, and the meaning and scope of rights under the Charter is the same as that under the Convention (see Article 52(3) of the Charter). The CJEU and the Court of Human Rights are also engaged in a "judicial dialogue" whereby they consider each other's judgments, sometimes cite to them, and meet regularly. Thus, there is mutual influence between the case law of the two courts.

At the same time, there is also tension between the Charter and the Convention, and between the two courts. The EU is legally obligated to accede to the Convention (Article 6(2) of the Treaty on European Union or TEU), but in 2014 the CJEU decided in *Opinion 2/13* that the accession treaty negotiated between the EU and the Council of Europe for the EU to accede to the Convention did not comply with EU law, so that at the moment the EU is not able to accede.

All this means that the DPAs and the EU courts take great account of both the Charter and the Convention in their work, since they have to, given the constitutional status of the Charter and its links to the Convention. This means that, for example, when interpreting the GDPR, they are legally required to take the Charter and the Convention into account, particularly in light of the high level of protection for personal data set out in the Charter (see, e.g., the CJEU's *Schrems* judgment, paras. 38-39). Since the CJEU has interpreted data protection law strictly, the practical impact of this is that DPAs tend to take a strict interpretation of the law based on the standards of the Charter and the Convention.

It is useful in this context to consider in more detail the Article 29 Working Party and the new European Data Protection Board ("**EDPB**") and their jurisdiction. The Article 29 Working Party is comprised of all the Member State DPAs together with the European Data Protection Supervisor ("**EDPS**"). It issues papers on numerous data protection topics that tend to be quite influential (see the Article 29 Working Party website), but which are not legally binding. Given that the Working Party will be replaced in approximately eight months by the EDPB, it is recommended to concentrate on the EDPB.

The jurisdiction of the EDPB is defined both territorially and substantively. The territorial jurisdiction of the EDPB is reflected in Article 3 GDPR, which is discussed in detail in our response to Question 13. The substantive jurisdiction of the EDPB is determined by the tasks it is given in the GDPR. Under Article 70, the EDPB has a large number of tasks which are too numerous to describe here. Most enforcement under the GDPR will likely still be carried out by the national DPAs, but the EDPB has the power to adopt legally binding decisions in certain cases involving enforcement. This is the case, for example, when different DPAs disagree about enforcement measures to be taken in multiple Member States (Article 65), or when a DPA believes that is necessary to take urgent action to protect data protection rights (Article 66). Thus, the EDPB will have an important role to play in data protection enforcement (see also our response to Question 14).

Neither the Article 29 Working Party nor the EDPB take into account foreign laws when ruling on a case. This reflects the emphasis in the GDPR on the fact that evaluation of data protection rights must be subject solely to EU or Member State law (see Articles 6(3) and 48 GDPR).

13. *In view of the borderless nature of the internet and the fact that European Union citizens may freely acquire domain names from registries and registrars in third countries, how could potential <u>conflicts of law</u> based on the current and future European Union data protection framework best be avoided?*

The broad territorial scope of EU data protection law has led to frequent legal conflicts with foreign requirements. The number of such conflicts is too numerous and the issues they present are too complex to describe here in detail. But some of the best-known such conflicts have involved the EU-US Safe Harbor arrangement; US whistleblowing requirements under the Sarbanes-Oxley Act; and US e-discovery requirements. In all these cases and many others, parties may be faced with the dilemma that compliance with EU data protection requirements may not always be compatible with requirements of third country laws.

The GDPR will likely lead to more such legal conflicts, since it has broad extraterritorial scope. Under Article 3, the GDPR applies to data controllers or data processors not established in the EU when their data processing activities are related to "(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union". These criteria are defined more precisely in the following recitals to the GDPR:

> Recital 23: "In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union".
>
> Recital 24: "[I]n order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes".

Of the two possible grounds for extraterritorial application of the GDPR under Article 3, the more likely one would seem to be "the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union". This would occur, for example, when registries and registrars offer their services to individuals in the EU via the Internet. Beyond legal application of the GDPR, it should be noted that it may also be applied extraterritorially through other means as well (for example, parties in the EU may require those in third countries to apply the GDPR as a condition for doing business with them).

There seem to be only two ways that such potential conflicts of law could be avoided: (1) the enactment of some sort of international agreement covering areas such as data protection, the

protection of intellectual property, and Internet governance, which would have to comply with the requirements of EU fundamental rights law; or (2) the harmonization of the above areas of law throughout the legal systems of the world. Since both of these possibilities are highly unlikely, at least in the short term, such conflicts are likely to continue.

A key reason why this is so is because of the overriding status that the CJEU has granted both EU law and the fundamental right to data protection when they conflict with other legal systems. The CJEU has made it clear that when EU primary law (such as fundamental rights) conflicts with foreign law (including international law), EU fundamental rights must be given priority (see the *Kadi* judgment, Joined Cases C-402/05 P and C-415/05 P, para. 285), and that this also applies in a case when EU data protection law is involved (see *Schrems*, paras. 86-87).

We think the best way to avoid conflicts would be to try to bring the data processing practices of ICANN and the registrars in line with EU data protection law as much as possible, and to give primacy to EU data protection requirements when they clash with those of other jurisdictions. However, we recognize that prioritizing compliance with EU data protection law may itself give rise to legal conflicts when EU law clashes with law and requirements in other jurisdictions. Thus, even this strategy cannot provide complete protection against such conflicts.

*14. Can the EU enforce provisions of the General Data Protection Regulation on ICANN itself, or just the EU Registrars and EU Registries? Will there be such enforcement?*

The EU is comprised of many different institutions, and only one of them is relevant to enforcement against ICANN under the GDPR, namely the new European Data Protection Board (EDPB). This is because the EDPB is the only institution of the European Union that is given the authority to supervise and enforce the GDPR. However, the national DPAs (which are independent supervisory authorities established at the national level, and not EU institutions) remain very relevant to enforcement of the GDPR.

Under the GDPR, the national DPAs will monitor and enforce its application within their territory (Article 57(1)(a)), and most enforcement actions will likely be brought by national DPAs. Individuals also have a right to a judicial remedy against data controllers and data processors (Article 79), so that there will be an increase in judicial enforcement of the GDPR.

The EDPB can issue binding decisions in cases where there are disputes between DPAs (e.g., when they disagree about whether there has been a violation of the GDPR) or when a DPA believes that urgent action needs to be taken to protect data protection rights. A binding decision of the EDPB will be an instrument of EU law that can be challenged in the EU courts.

Both the national DPAs and the EDPB will have jurisdiction over all types of entities (including registries, registrants, registrars, etc.) that are within the GDPR's material and territorial scope. As explained in the response to Question 13, the GDPR has extraterritorial scope, so that they can take enforcement action with regard to activities performed outside the EU. However, the DPAs and the EDPB may not directly enforce EU data protection law outside the territory of the EU.

Whether ICANN itself would fall under the jurisdiction of European DPAs or courts is determined by its corporate structure and presence in Europe, about which we do not have sufficient information to give an opinion. However, it is possible that ICANN could be found liable in the EU for activities outside the EU. In *Google Spain* the CJEU held that because the activities of Google's European affiliates were "inextricably linked" to the operation of the Google search engine run by the Google parent company in the US, the search engine was subject to EU data protection law. The CJEU stressed in particular that the two were inextricably linked because the activities of Google's European affiliates allowed the operation of the search engine by the Google parent to be economically profitable (see para. 56). We cannot evaluate here whether such an argument would apply to ICANN and the registries, but it should be kept in mind.

It should also be noted that the DPAs are active in multinational data protection enforcement networks (such as the Global Privacy Enforcement Network initiative of the OECD), and may also attempt to obtain extraterritorial enforcement that way as well.

**Compliance with Applicable Laws**

15. *Article 6 of the General Data Protection Regulation provides that processing is lawful if, among other things, the processing is "necessary to protect the vital interests of . . . another natural person or for the legitimate interests pursued by . . . a third party." Under these principles, and given the longstanding and historical use of registration data made available through WHOIS as a de-facto public resource, do you agree this information should continue to be made readily available to those who investigate fraud, consumer deception, intellectual property violations, or other violations of law?*

Please note that the quotation above is incorrect: Article 6(1)(d) provides a legal basis when "processing is necessary in order to protect the vital interests of the data subject or of another natural person", and Article 6(1)(f) does so when "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party…". The language quoted above seems to be a mixture of these two provisions; therefore, we will discuss both of them.

Article 6(1)(d) would not apply to the investigation of IP violations and other related acts, since the vital interest legal basis applies only when data processing is necessary to protect an interest that is essential for the life of the data subject or another natural person (see GDPR Recital 46). This means that the term "vital interest" is to be interpreted as referring to an individual's life, health, safety, or other such interest that is essential to their physical well-being.

With regard to Article 6(1)(f), the full provision reads "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". Thus, in interpreting Article 6(1)(f), it is essential to weigh the legitimate interests of the data controller against the fundamental rights and freedoms of the data subject. As stated

above, the CJEU has ruled in the *Google Spain* case that serious interference with an individual's data protection rights cannot be justified by the economic interest of a search engine operator (para. 81). Also, the CJEU has ruled that a filtering system to prevent copyright infringement may infringe the data protection rights of the ISP's customers as it involves a systematic analysis of all content and the collection and identification of users' IP addresses from which unlawful content on the network is sent (*Scarlet Extended SA v SABAM*, Case C-70/10, paras. 50-51). The CJEU has also recently ruled again that review of limitations on data protection rights must be strict (*Opinion 1/15*, para. 140).

With regard to the "legitimate interests…pursued by a third party", the conditions for applying this are the same as for interpreting the legitimate interests of the data controller. In its 2014 opinion on the interpretation of Article 7(f) of the Data Protection Directive, the wording of which is nearly identical to Article 6(1)(f) of the GDPR, the Article 29 Working Party indicated that one such legitimate interest pursued by a third party could include combatting "illegal file sharing online" (WP 217, pp. 28-29).

The above discussion means that use of WHOIS data could be seen as pursuing a legitimate interest of a data controller or a third party. However, the existence of a legitimate interest is not enough to justify data processing: rather, the legitimate interest must be balanced against the fundamental rights and freedoms of the individuals whose data will be processed. Particularly important in this balancing test are the impact on data subjects (which includes factors such as the nature of the data, and the way the data are processed); factors such as proportionality and transparency; and any additional safeguards applied by the data controller (WP 217, pp. 33-42).

Question 15 seems to assume that WHOIS data would be made readily available, in large quantities, to a broad spectrum of parties, for broad purposes, and in ways that will not always be transparent to individuals. In light of these considerations, we believe that the conditions for using the "legitimate interests" legal basis would not be satisfied, whether the legitimate interest pursued is that of the data controller or of a third party.

16. *Our working group deals with policies pertaining to generic top-level domains (gTLDs). However, each country establishes its own policies pertaining to country-code top-level domains (ccTLDs). Currently, all EU states have ccTLD registries which provide publicly available registration data through WHOIS, both for private individuals and commercial entities. Can you explain how these ccTLD registry policies are able to comply with EU data protection laws?*

In order to respond to this question, it would be necessary to review the ccTLD policies under national data protection law, and to have the full background of how the policies were drafted, details of any interactions between the registries and their national DPAs, and similar information. This is because national data protection laws vary widely, and it is likely that the compliance policies vary also country by country. We do not have access to such policies, and reviewing them for compliance with EU law would far exceed the scope of this memorandum.

We would like to reiterate our view that since the GDPR will come into force in less than a year, it is imperative that ICANN orient its policies and practices around that rather than national laws.

17. *The gTLD ecosystem includes the Generic Names Supporting Organization which recommends policy, ICANN which implements that policy, registries which administer the domain name space under a given gTLD, and registrars which register domain names for use by registrants. Within this ecosystem, who do you see as the data controller, in terms of the EU definitions of data controller and data processors?*

The data controller is the entity that decides the purposes and the means of the processing, and a data processor conducts the processing exclusively on behalf and at the instruction of the data controller. Where one or more entities decide the purposes, they may be joint controllers. It is also possible that the same entity is a controller for one purpose, and a processor for another. As the purposes have not yet been formulated, it is not yet possible to conclusively assign the roles, but we can give some guidelines.

The concept of data controller is a functional concept, intended to "allocate responsibilities where the factual influence is, and thus based on a factual rather than formal analysis" (Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (WP169), p. 9). Following this criteria of factual influence, ICANN is a data controller to the extent that it autonomously decides and imposes its policy on the other entities involved. Similarly, to the extent that a national registry is free to make its own policy with regard to processing of data in the context of its ccTLD, it may be an independent controller. If the factual influence can be exhaustively allocated between the various autonomous entities, without any overlapping competences, then there will be one independent controller for each purpose, and each entity will be either a controller or processor for their part. However, we understand that there may be considerable overlap of authority, or at least of factual influence.

It is impossible to set out here how the data controller would be determined for each WHOIS field, since that would involve an evaluation of the complexities of how data are collected and used for each field, and would exceed the scope of this memorandum. Generally speaking, we believe that the best view would be to see each of these entities as a co-controller, i.e., each of them would be regarded as data controller. This is the case for the following reasons:

- As set forth in the question, it seems that each of them has a role in determining the purposes and means of data processing in the domain name ecosystem. Under Article 4(7) GDPR this means that registries, registrars, or any other parties that determine the purposes and means of how data will be processed in the domain name system could each be a data controller.
- The *Google Spain* case illustrates that the CJEU tends to find that each of the parties involved in running highly complex online systems are data controllers.

- Courts and DPAs in the EU tend to be suspicious of allowing such parties to be classified as data processors, since most legal responsibility rests with the data controllers.

The fact that all these parties would act as joint controllers means that under Article 26(1) GDPR, ICANN and the registrars should implement an "arrangement" to govern matters such as "their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14" (Article 26(1)). This could be done through revisions to the policies and procedures that determine the relations between ICANN and the registrars.

Thus, being found to be joint controllers need not have negative ramifications, as long as ICANN and the registrars come to an agreement to organize their respective relations in accordance with the GDPR. We also recommend that a DPIA be conducted with regard to the data collected in each particular field, in order to evaluate the data protection implications of such data collection and determine how they could be best dealt with.

**Consumer Protection**

18. *Can you comment on your understanding of the need for owners of trademarks/brands and IP to avoid and combat infringement, and this need's connection to consumer protection, in the context of the EU ePrivacy Directive and the General Data Protection Regulation?*

As this question seems to us a repetition of Question 9, we refer to our answer there.

19. *Today, intellectual property and trademark rights holders depend on registration data obtained through the WHOIS directory service to police the misuse of their intellectual property on commercial websites, track down purveyors of counterfeit goods, and prevent fraudulent websites from engaging in illegal activity on the Internet. Is creating a repository of information for contactability to facilitate reaching those business registrants a valid purpose for this directory service and, if not, why not?*

We have extensively addressed issues of purpose limitation already in this memorandum (see for example the response to Question 1), and will not repeat the legal analysis we gave there, which applies to this question as well. That is, creating a repository for contactability may be in itself a legitimate purpose, but it depends on how this purpose would be implemented, and what the legal basis for it would be. The fact that contactability is involved rather than some other purpose would not change the legal analysis. It is likely that consent would be needed as a legal basis, and thus the requirements for valid consent set out in the answer to Question 11 would have to be fulfilled. The threshold for the valid use of consent is high, and probably separate consent would need to be obtained for contactability.

* * *