hamilton

MEMORANDUM

To	Internet Corporation for Assigned Names and Numbers
From	Thomas Nygren and Pontus Stenbeck, Hamilton Advokatbyrå
Date	16 October 2017
Subject	gTLD Registration Directory Services and the GDPR - Part 1

1. BACKGROUND, SCOPE AND STRUCTURE

1.1 In its preparations for the entering into force of the EU General Data Protection Regulation 2016/679 (the "**GDPR**") on 25 May 2018, the Internet Corporation for Assigned Names and Numbers ("**ICANN**") has requested Hamilton Advokatbyrå to provide an independent assessment of the legal challenges that the GDPR will entail in relation to the registration directory services for generic top-level domains ("**gTLDs**"), commonly known as Whois, that is made available to the general public on the requirement of ICANN, as further described in section 2 below.

1.2 Our assignment focuses on the processing of data which ICANN currently requires registrars (accredited by ICANN) and registries (registry operators) to obtain from domain name registrants ("**Whois data**"), in particular personal data, which is being maintained by registrars and registries in different directories and made publicly available through so-called look-up tools (any services provided in relation to Whois data are herein jointly referred to as "**Whois services**"). Our analysis will primarily be based on the preferred option of ICANN for the Whois services to remain in their current state following the GDPR entering into force. For the avoidance of doubt, it should be noted that our analysis will only cover directories, and related services, for gTLDs, excluding for instance country code top-level domains ("**ccTLDs**"), and the terms "Whois services" and "Whois data", as used in this memorandum, only comprise services and data relating to gTLDs, as carried out based on the contractual requirements in the agreements between ICANN and registrars and registries.

1.3 Due to the complexity of the issue, we intend to provide a series of memorandums, which will address different aspects of the issue and where the

scope and topics of each such memorandum will be discussed and agreed with ICANN. We understand that ICANN intends to make each memorandum publicly available.

1.4 As basis for our analysis, ICANN has provided us with a first set of questions, attached hereto as Appendix 1, and we will aim to address these questions, as appropriate, in our memorandum series, although our analysis will not be limited to the scope thereof.

1.5 While our memorandum series will primarily focus on the GDPR, we will also address other relevant pieces of EU legislation that may have effect on the processing of personal data through the Whois services, such as but not limited to the EU ePrivacy Directive 2002/58/EC and the proposed new EU ePrivacy Regulation aimed to replace the said directive in May 2018.

1.6 This first memorandum will mainly focus on describing the main issues that the GDPR will give rise to in relation to the Whois services in their current form, and on how the processing of personal data through the Whois services, as carried out today, would comply with the requirements of the GDPR. This memorandum will also address the questions raised by ICANN in Appendix 1 on a general level, while assessing some of them in more detail where appropriate for the main purpose of this memorandum (i.e. assessing the general compliance with the GDPR of the data processing currently entailed by the Whois services). This memorandum does not intend to exhaustively answer all the questions in Appendix 1 in detail but rather to use the questions to provide a general background description of the regulation before discussing certain main issues on a more detailed level.

1.7 The subsequent papers in our memorandum series will focus more on how the philosophy and thinking behind the Whois services, as well as the view of the Whois services from a legislative and regulative perspective, could possibly be changed to allow the services to remain and evolve under the GDPR.

2. WHOIS DATA PROCESSING

2.1 In 2009, ICANN was assigned by the United States Department of Commerce (the "**USDC**") under an Affirmation of Commitments (the "**AoC**") to institutionalize and memorialize the technical coordination of the internet's domain name and addressing system. Among other things, the AoC included a commitment for ICANN to enforce its then existing policy relating to the Whois services, including to "maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information".

2.2 As a final part of the process of separating ICANN from the United States government, the USDC and ICANN mutually agreed to terminate the AoC in January 2017, after the material framework of the AoC had been incorporated in ICANN's bylaws. Under the bylaws, ICANN shall, subject to applicable laws, "use commercially reasonable efforts to enforce its policies relating to registration directory services" and "cause a periodic review to assess the effectiveness of the then current gTLD registry directory service and whether its implementation meets the legitimate needs of law enforcement, promoting consumer trust and safeguarding registrant data".

2.3 Under an accreditation agreement that ICANN enters into with each of its accredited registrars, the 2013 Registrar Accreditation Agreement (the "**2013 RAA**"), and the agreement that ICANN enters into with each registry (the "**Registry Agreement**"), ICANN requires that the registrars and registries collect certain data regarding any registered domain name and the registrants of such domain names and that the collected data is made publicly available through the Whois services. Under both the 2013 RAA and the Registry Agreement, the registrar, who is the party responsible for obtaining the requested data from the domain name registrants, is obligated to obtain consent from each registrant for the requested data processing.

2.4 The data required under the 2013 RAA to be collected and made available through Whois services includes:

(i) the registered domain name;

(ii) the names of the primary nameserver and secondary nameserver(s) for the registered domain name;

(iii) the identity of registrar;

(iv) the original creation date of the registration;

(v) the expiration date of the registration;

(vi) the name and postal address of the domain name registrant;

(vii) the name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the registered domain name; and

(viii) the name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the registered domain name.

2.5 In addition to the data types set out in section 2.4 above, the 2013 RAA allows for the registrar to add additional data elements as well.

2.6 Although the Whois services offer certain ways for registrants to keep information restricted from public access, such as proxy options, the default setting is that the registration data obtained is made publicly available.

3. GDPR DESCRIPTION AND APPLICATION

3.1 Status and Implementation

3.1.1 The GDPR enters into force on 25 May 2018 and will from then on, as an EU regulation, apply as law with direct effect in all EU member states without the need of national implementation legislation. Notwithstanding the foregoing, the GDPR leaves some elements (such as a right to add additional sanctions) for the member states to decide and implement on member state level through national legislation and there can thus be expected to be some minor national differences. Further, the different history and tradition of data protection law within the European Union is likely to cause some difference in interpretation among the member states, in particular during an initial period.

3.1.2 When entering into force, the GDPR replaces the current EU Data Protection Directive 95/46/EC, (the "**Data Protection Directive**") and any EU member state legislations based on the Data Protection Directive. The GDPR is to a large extent based on the same principles as the Data Protection Directive, but with more focus on protecting the integrity of individuals. Other, notable, differences are increased and stricter requirements for controllers and processers and a significantly more extensive and severe sanctions catalogue.

3.2 Territorial Application

3.2.1 The GDPR has extended territorial scope compared to the Data Protection Directive and Article 3 GDPR sets out that it, in addition to being applicable to controllers and processors established in the EU, will apply to controllers and 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".

3.2.2 Extraterritorial reach as described in section 3.2.1 above will apply, for instance, when registrars and registries established outside the EU provide their domain name registration services to natural persons in the EU.

3.2.3 The national data protection authority of each EU member state (each a "**DPA**") will monitor and enforce the GDPR within its respective territory and the DPAs are expected to carry out most of the enforcement actions under the GDPR. Correspondingly, each EU member state's national courts will have the jurisdiction to enforce the GDPR in its respective territory.

3.2.4 Another body that plays a central role in the interpretation of the GDPR is the Article 29 Working Party, which is an advisory and independent working group consisting of representatives from all DPAs, the European Data Protection Supervisor and the EU Commission. The Article 29 Working Party issues guidelines and opinions in relation to data protection issues, which are not legally binding but nonetheless influential. When the GDPR enters into force in May 2018, the Article 29 Working Party will be replaced by a new European Data Protection Board (the "**EDPB**"), which is established under Article 68 GDPR as an independent body of the Union and is given a number of tasks set out in Article 68 GDPR. Among its authorizations, the EDPB will have the right to issue binding decisions in case of disputes between the DPAs.

3.3 Transfer of Personal Data to Third Countries

3.3.1 There are no restrictions *per se* under the GDPR on the transfer of personal data from one EU member state to another. However, the transfer must be in compliance with the GDPR (i.e. the transfer must be covered by the determined purpose of the processing, the data subject must have been duly informed etc.). It should also be noted that a transfer between two different legal entities requires the parties to take safety measures to ensure that the data subject's rights are upheld (a request for the right to be forgotten would for instance require the controller to take effort to ensure that personal data is cleansed by other legal entities).

3.3.2 According to Article 45 GDPR, a transfer of personal data to a third country (i.e. a country which is not a member of the EU or the European Economic Area) may take place without requiring any specific authorization where the EU Commission has decided that the third country ensures an adequate level of protection.

3.3.3 If the receiving country is not deemed ensure an adequate level of protection, the transferring party has to implement appropriate safeguards, as listed in Article 46 GDPR. As of the date of this memorandum several of the safeguards listed therein

have yet to come into existence (i.e. standard data protection clauses adopted by a DPA, approved codes of conduct and approved certification mechanisms) and the actual availability of such safeguards can be expected to change in the future.

3.3.4 Article 46(c) GDPR allows for transfer to a third country if standard data protection clauses adopted by the EU Commission are applied. These clauses can be made part of an agreement, and could for instance be included in the accreditation agreement between ICANN and the registrars, in order to ensure the legality of third country transfers. However, it should be noted that the existing model clauses recently have been subject to criticism and that their validity is to be tried by the Court of Justice of the EU (the "**CJEU**"). Their future validity, at least in their current form, is therefore somewhat uncertain.

3.3.5 It is also possible for parties transferring personal data to enter into contractual clauses that are not standardized. However, this is only considered an appropriate safeguard under the GDPR if such contractual clauses have been authorized by a DPA. In light of the foregoing, the only safeguard what would currently be available for ICANN in practice, and which does not require authorization from a DPA, is the use of EU Commission standard clauses.

3.3.6 As regards transfer of personal data from the EU to the United States, such transfers are allowed under the Privacy Shield regime. Under Privacy Shield, the EU recognizes that any United States organization that joins Privacy Shield is deemed to have an adequate level of protection. Consequently, if a receiver of personal data is certified under Privacy Shield, no safeguards under Article 46 GDPR are necessary. Whether the validity of Privacy Shield will be challenged under the GDPR is yet to be seen but until further notice, Privacy Shield allows for transfers to the United States.

3.4 Accountability

3.4.1 Article 5 GDPR sets out a set of ground principles for processing of personal data (of which some are described in more detail below) and requires the controller to be responsible for, and able to demonstrate, compliance with the said principles (accountability).

3.4.2 In short, the accountability principle requires the controller to:

(i) implement appropriate technical and organizational measures (for instance by implementing internal policies) to ensure compliance;

(ii) thoroughly document such measures; and

(iii) periodically review and update such measures where necessary.

3.4.3 Further guidance on the implementation of appropriate measures and the demonstration of compliance, including on how to identify, assess and mitigate risks associated with data processing, is to be expected from the Article 29 Working Party and, after its establishment, the EDPB.

3.4.4 In relation to the accountability principle, the GDPR encourages, and requires in cases where a processing activity is "likely to result in a high risk to the rights and freedoms of natural persons", controllers to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment ("**DPIA**")). Where a DPIA is required for a processing activity for which there are joint controllers (as further described in section 3.7 below), a DPIA would have to be carried out by all joint controllers. Given the scale and complexity of the processing activities carried out in relation to the Whois services, including for instance the processing of data outside of the European Union, we would recommend ICANN to conduct a DPIA with regard to ICANN directing the processing of data within the scope of the Whois services (see section 3.7.2 below). Although the scope of this DPIA needs to be assessed separately, and is not included in our analysis in this memorandum, we envision it to be carried out by ICANN alone, in its capacity of controller on the "top level" (as compared to registrars and registries possibly being deemed to be controllers for certain parts of the processing further down in the value chain, as further discussed in sections 3.7.2 and 3.7.3 below).

3.5 Personal Data and Processing

3.5.1 Under the GDPR, "personal data" is defined as "any information relating to an identified or identifiable natural person (a data subject)". Consequently, data processed through the Whois services will not be covered by the GDPR if it relates solely to a legal person.

3.5.2 As illustrated in section 2 above, the Whois services comprise a number of different types of data which are made available to the public. Some of this data is clearly personal data (e.g. the name and address of a natural person) and some is clearly not personal data (e.g. company names which do not include any name of or other tie to an identifiable natural person) while other data does not

immediately seem to qualify as personal data (e.g. server name) but may, depending on the context, still be possible to tie to a natural person, thus constituting personal data. Even if the information relates only to a legal person, it would still constitute personal data if, for instance, the company name includes the name of an identifiable natural person, if the contact address is a natural person's residence or if the e-mail contact address contains the name of a natural person.

3.5.3 It is without doubt that a large portion of the data being made publicly available through the Whois services will constitute personal data under the GDPR, although it might be difficult to make a general categorization of whether a certain data type would always constitute personal data.

3.5.4 "Processing" of personal data under the GDPR is defined as "any operation or set of operations which are performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". For instance, both the collection of data from a registrant and the displaying of data in a Whois look-up tool constitute different processing activities under the GDPR.

3.6 Data Processing Purposes

3.6.1 Under Article 5 GDPR, personal data may only be processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The controller is responsible for formulating the purpose of any processing of data and is obligated to inform any data subjects of such purpose before commencing the processing. The providing of such information is further a prerequisite for obtaining consent for processing (as further described below).

3.6.2 A processing activity can have several different purposes. Each such purpose then requires its own legal ground (as further described below) and all legal requirements (including but not limited to the obligation to inform the data subjects) must be fulfilled for each purpose. Further, Article 25 GDPR sets out that only personal data which is necessary for each specific purpose shall be processed (data protection by default).

3.6.3 Article 5 GDPR sets out that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization). As will be further discussed in this memorandum, it can be

questioned if all the data being made available through the Whois services is necessary in relation to the purposes for which the data is collected.

3.6.4 From an outside perspective, the purposes of the data processing within the Whois services are currently not entirely clear and transparent. Looking at the communication surrounding the Whois services, it was originally focused on using registrant data for technical contacts, while the current ICANN bylaws emphasizes on law enforcement and consumer rights. In this context, the commitment to the USDC under the now terminated AoC, as described in section 2.1, to provide unrestricted and public access to registrant data should also be mentioned.

3.6.5 In order for the Whois services to function under and comply with the GDPR, it will be imperative to determine and define the purposes for processing. Having identified the intended purposes will in turn facilitate determining which data to process and how to process it and is an important part of being able to comply with the GDPR.

3.7 Data Controller

3.7.1 According to Article 4(7) GDPR, a "controller" of personal data is an entity which alone or jointly with others, determines the purposes and means of the processing of personal data. Where several entities are jointly determining the purposes and means of the processing, they are considered to be joint controllers. It is further possible for an entity to be controller for one purpose and processor (i.e. an entity that process data on behalf of the controller) for another, within the scope of the same processing.

3.7.2 With regard to the personal data processing carried out in relation to the Whois services, different parties can be the controller for different processing purposes. For instance, ICANN is for sure to be considered as the controller in the context that it requires registrars and registries to obtain certain data and, through its agreements and policies, directs the processing of data within the scope of the Whois services. However, we understand that registrars and registries may control certain parts of the processing on their own, for instance where a registrar chooses to obtain additional personal data, which could make them the controller with regard to certain processing.

3.7.3 While it in theory might be possible to determine which party of ICANN, a registrar and a registry is the controller of any given processing of personal data within the framework of the Whois services, this will most likely be a difficult exercise in practice, as the parties have different influence over different parts of the processing. In light hereof, our recommendation would be to take the general

approach that the involved parties are all considered to be joint controllers. This view would help mitigate the risk that a DPA makes a different assessment but would also offer a practical solution to the issue.

3.7.4 Where there are two or more controllers, Article 26 GDPR sets out that these shall adopt an arrangement setting out their respective roles and obligations in relation to the processing. This could for instance be achieved through amending the relevant agreements and policies regulating the relationship between ICANN and the registrars and registries.

3.8 Legal Grounds for Processing

3.8.1 General

3.8.1.1 Article 5 GDPR sets out that any processing of personal data must be lawful. Processing of personal data is considered lawful, and hence permitted, under the GDPR only if at least one of the legal grounds set out in Article 6.1 GDPR is applicable.

3.8.1.2 Of the legal grounds referred to above, the ones that primarily could be relevant for the Whois services are consent (Article 6.1(a) GDPR), necessity for the performance of a contract (Article 6.1(b) GDPR) and legitimate interest (Article 6.1(f) GDPR).

3.8.2 Consent

3.8.2.1 According to Article 6.1(a) GDPR, processing is lawful when the data subject has given consent to the processing for one or more specific purposes.

3.8.2.2 As mentioned above, the processing of personal data through the Whois services is currently based on the consent of the registrants, and the registrars are contractually bound to ICANN to obtain such consents. The consents are worded and obtained by the registrars and we understand, without having reviewed the consent wordings currently used by registrars on a large scale but given the large number of accredited registrars, that the existing consents probably vary in both scope and language.

3.8.2.3 While consent will continue to constitute a legal ground for processing under the GDPR (as is the case under the Data Protection Directive), the prerequisites for consent will change to some extent compared to today and any consent obtained will need to fulfil the following requirements:

(i) The consent must be specific and unambiguous and shall be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Any consent should therefore be separate from any other consent or description of personal data processing, so that it is clear what the registrant consents to.

(ii) The consent must be informed, meaning that the purposes of the processing that are subject to the consent are clearly described before the consent can be given. If several different purposes require consent, the consent should be given for each of those purposes separately, giving the registrant the option not to give consent.

(iii) The consent must be voluntary and freely given by a statement or a clear affirmative action. According to Article 7.4 GDPR, when assessing whether the consent is freely given, "utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract". The consequence of this provision is not entirely clear but should mean that it would normally not be possible to condition the validity of a contract upon consent for a purpose which is not necessary for the performance of the contract. For instance, if it is established that it is not deemed necessary for the registration of a domain name to make all information regarding the registrant publicly available, it would not be compliant with Article 7.4 GDPR to make the registration conditional upon the registrant's consent to have its information publicly published through the Whois services. Consequently, a registrant should be able to register a domain name without having to consent to any processing of personal data other than the processing that is necessary to perform the agreement. The fact that the only way to obtain and register a domain name under, for instance, a .com gTLD is to use channels accredited by ICANN should also be factored in when assessing whether the consent is in fact freely given.

(iv) The registrant must be able to withdraw the consent at any time. The registrant must be informed of this withdrawal right before giving the consent and it should be as easy to withdraw as to give the consent. Further, technical and operational procedures must be implemented which allows for withdrawal of consent in an efficient manner.

3.8.2.4 Consents obtained under the Data Protection Directive will continue to apply under the GDPR only if they are compliant with the new rules. In practice, this means that most consents currently existing will have to be replaced.

3.8.2.5 It should be noted that consent models can be found in national legislation regarding ccTLDs. As comparison, the Swedish Act on National Top-Level Domains for Sweden on the Internet (*Sw. lag (2006:24) om nationella toppdomäner för Sverige på Internet*), which governs the allotment and registration of domain names under the ccTLD for Sweden, namely .se, (and which thus is not applicable on gTLDs) also regulates the provision of a domain name directory. The publication of personal data in such directory is subject to the provisions of the Swedish Personal Data Act (*Sw. personuppgiftslagen (1998:204)*), which is the Swedish implementation of the Data Protection Directive, and to the consent of any registrants being natural persons.

3.8.3 Performance of a Contract

3.8.3.1 According to Article 6.1(b) GDPR, processing is lawful when necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

3.8.3.2 It can be argued that some processing of personal data, such as the need for the registrars to be able to contact the registrants for invoicing, support and other purposes connected to the administration of a domain name, is necessary for the registrar to perform its contract with the registrant. This need would however not extend to making the data available to the public.

3.8.3.3 As ICANN is not party to any agreement with registrants, the direct application of performance of contract as legal ground might be limited, but the fact that some processing will be required by the registrars for performance of the 2013 RAA should in any case be possible to factor in as a legitimate interest (see section 3.8.4 below).

3.8.4 Legitimate Interest

3.8.4.1 According to Article 6.1(f) GDPR, processing is lawful when necessary for "the purposes of the legitimate interests pursued by the controller or 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".

3.8.4.2 For this legal ground to apply, it is not sufficient that a legitimate interest exists, but it must be weighed against, and override, the fundamental rights and freedoms of the data subject, and this is up to the controller to demonstrate. This weighing of interests need to take a number of elements into account, in particular relating to the impact on the data subject, such as the type of data being processed and the way it is being processed and the proportionality and transparency of the processing. An illustration of the limitations of legitimate interest as legal ground for processing (under the Data Protection Directive) can be found in the *Google Spain* case from the CJEU, C-131/12 (para. 81), where it was established that serious interference with an individual's data protection rights cannot be justified by the economic interest of a search engine operator.

3.8.4.3 Looking at the current Whois services, there are several fields of use that could potentially qualify as legitimate interest. For instance, recital 47 GDPR specifically mentions processing necessary for preventing fraud as a legitimate interest and the Article 29 Working Party has indicated that the "combatting of file sharing" could constitute a legitimate interest. In line herewith, it can be argued that the following purposes of processing could constitute legitimate interest under Article 6.1(f) GDPR:

(i) The use of Whois data, for instance by registrars and network operators, for invoicing, support and other administration actions in relation to registered domain names.

(ii) The use of Whois data to investigate fraud, consumer deception, intellectual property violations, or other violations of law.

(iii) The use of Whois data to verify the identity of a provider of goods or services on the internet, including for consumer protection purposes.

(iv) The use of Whois data to identify the owner of a domain for business purposes, for instance in relation to a purchase of the domain name or other transactions.

3.8.4.4 Although it can be argued that each of the usages listed above could qualify as a legitimate interest, it must, in relation to the weighing against fundamental rights and freedoms of the data subjects, be taken into account that the Whois data is currently being made available to the general public, in large quantities and that the data can be used for other purpose than the ones listed above or otherwise intended, with very limited means of control for the controller.

3.8.4.5 In historic correspondence with ICANN, the Article 29 Working Party has expressed that it acknowledges the use of Whois services for support purposes as a legitimate purpose but that the public access to the Whois data in its current form goes beyond that legitimate purpose. This reasoning is very much in line with the opinions expressed by CJEU case law and the actions of the DPAs.

3.8.4.6 According to Article 21 GDPR, the data subject has a right to object to processing based on legitimate interest. In the event of such objections, the controller must be able to demonstrate *compelling legitimate grounds* (a slightly higher threshold) for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

3.8.5 Conclusion

3.8.5.1 With the view currently applied by the EU data privacy community (including legislators, courts and authorities) on large quantities of personal data being made available through public directories on an unfiltered basis, our assessment is that it will not be possible to claim legitimate interest as a legal ground for processing of personal data as currently performed through the Whois services on an unchanged basis.

3.8.5.2 Both legitimate interest and necessity for performance of a contract, or a combination thereof, could most likely be used as legal ground for some of the purposes of the Whois services, but cannot, as the existing purposes are phrased and with the current view of the EU data privacy community, serve as a legal ground for the current public accessibility of the Whois data.

3.8.5.3 In our opinion, the current open, publicly available Whois services can only remain on an unchanged basis, i.e. as currently provided by processing the same types and quantities of data in the same way as today, if any processing of personal data carried out in connection therewith is based on consent. As discussed above, this would however be a complex solution, entailing a number of technical and organizational challenges, and is unlikely to solve all issues, especially since the Whois services, with regard to personal data, will be dependent upon the registrants providing, and withdrawing, their consents.

3.9 Finding New Ways Forward

3.9.1 As illustrated above in this memorandum, there is no quick and easy way for moving forward with the Whois services in their current form. Instead, we suggest that this issue is approached from several different angles.

3.9.2 In our opinion, a natural starting point would be for ICANN to evaluate and determine the purposes for processing and assess to which extent personal data need to be processed for each purpose. If law enforcement is identified as a purpose, it might for instance be sufficient that the registrars keep full record of the complete registrant information, with a right for law enforcement agencies to access such records but without making them publicly available.

3.9.3 Our belief is that several of the purposes for which the data currently is processed (such as law enforcement, technical support and invoicing) could be achieved by using a layered model where the data necessary for a certain purpose can be accessed by the parties that actually need it, and that such a layered model probably could be based on legitimate interest or necessity for performance of contract (or a combination thereof).

3.9.4 We expect that an assessment in accordance with sections 3.9.2 and 3.9.3 would probably result in ICANN ending up with certain types of data that it wishes to continue to make publicly available through the Whois services, although we think that this data, and the processing thereof, could be less extensive and intrusive than what is the case today without affecting the quality of the services (it could for instance be discussed whether it is necessary to publish the phone number of natural persons). In our next memorandum we will examine to what extent this could be achieved by applying the legal grounds offered under the GDPR and, in particular, explore whether legitimate interest could potentially be used as legal ground for such processing in light of the current views in the data privacy community on public directories, and by drawing comparisons to other types of public directories which are considered lawful. We will also examine how a purpose for processing data in a public directory could be formulated.

_____

APPENDIX 1

Questions for GDPR Legal Analysis (External)
29 August 2017

ICANN is in the process of engaging legal experts to analyze the impact the European Union General Data Protection Regulation ("GDPR") will have on various data processing activities under ICANN policies and contracts. Such policies and contracts require or permit various entities that participate in the gTLD domain name system, including registries and registrars, to collect, create, retain, escrow, and publish a variety of personal data elements related to registry/registrar operations, domain name registrations, and registrants.

The legal review and analysis is proposed to be conducted in iterative phases, and will address questions such as the following:

1. What is the general status of the GDPR and implementation by EU Member States?
2. What are the major changes from the current EU Data Protection Directive and Member State implementation legislation?
3. What elements of domain name registration data constitute personal data (e.g. IP address, Server Name, etc.) under the GDPR?
4. When and how does the GDPR apply to personal data processing related to the domain name system functions? As a comparison, are telephone books permissible in the EU; would sending them outside the EU be a violation of the GDPR?
5. Is there a difference between an entity retaining data and another displaying it?
6. What is the extraterritorial application and reach of the GDPR?
7. What are the roles of "processors" and "controllers" under the GDPR and how does this apply to the various participants and processing activities in the domain name system?
8. How does the concept of "legitimate interest" apply to the processing and publishing of domain name registration data? Can the purpose of data retention be a justification for an exemption (e.g. registration data escrow)?
9. How can data subject consent requirements be applied to domain name registration data processing and publishing?
10. Are there restrictions on transfers of personal data between different jurisdictions within the EU? What are the restrictions on transfers to third countries and applicable derogations as they relate to domain name registration data?
11. What is the role of the EU-US Privacy Shield as it relates to the various data processing activities under ICANN policies/contracts and GDPR?
12. What are the GDPR's accountability and privacy management requirements, and how do they apply to domain name registration data?
13. What is the relevance the role of guidance from various relevant authorities (e.g. local data protection authorities, courts, Article 29 Working Party, etc.)?
14. What are the implications of any Member State implementation legislation to such requirements?

15. How should ICANN consider engaging with regulators regarding implications of GDPR on various data processing activities under ICANN policies and contracts?
16. How should the uses of domain name registration data as contributed by the ICANN community be analyzed in light of GDPR requirements? How do the use cases contributed by the ICANN community align with GDPR requirements?
17. What measures could ICANN, registries and registrars take to address any issues identified in the above questions?