hamilton

MEMORANDUM

To	Internet Corporation for Assigned Names and Numbers
From	Thomas Nygren and Pontus Stenbeck, Hamilton Advokatbyrå
Date	15 December 2017
Subject	gTLD Registration Directory Services and the GDPR - Part 2

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.

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 memoranda, 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 On 16 October 2017, we published part 1 of our memoranda series (the "**October 2017 Memorandum**"), which focused on the compliance of the Whois services, in their current form, with the GDPR.

1.5 In this part 2 of our memoranda series, we will address certain questions that have been raised by the gTLD community and provided to ICANN following the publishing of the October 2017 Memorandum. This memorandum will aim to answer most of these questions on a brief and general basis, in order to provide an increased general understanding of the GDPR.

1.6 Several of the questions provided require more elaboration and discussion and form a natural part of our ongoing assessment of whether the Whois services could possibly be changed in order to become compliant with the GDPR. This further assessment will be presented in part 3 of our memoranda series, which is to be published during December 2017.

2. ANSWERS TO COMMUNITY QUESTIONS

2.1 Please clarify the territorial scope of the GDPR. For example, would the GDPR apply to the processing of personal data of a French citizen who lives in Canada?

2.1.1 Article 3 GDPR sets out that it is primarily applicable on processing of personal data carried out by data controllers and processors established in EU. Therefore, all processing of personal data is, no matter where it is carried out, within the territorial scope of the GDPR as long as the controller or processor is considered established within the EU; the nationality, citizenship or location of the data subject is irrelevant.

2.1.2 In order for a controller or processor to be considered established in the EU it is not necessary for a controller or a processor to be incorporated in an EU member state; it is only required that there is some manner of effective and real exercise of activity through stable arrangements, e.g. a branch or a subsidiary. For instance, although we have not investigated this issue in detail, it is possible that ICANN could be considered to have an establishment in the EU through its corporate presence in Belgium.

2.1.3 In addition, the territorial scope of the GDPR is extended to also encompass any processing carried out by controllers or processors not established in the EU under certain circumstances, e.g. when a controller actively offers its goods and services to data subjects located within the EU. The applicability of the GDPR on controllers

and processors not established in the EU are further explained in section 3.2 of the October 2017 Memorandum.

2.1.4 In summary, it is the establishment or business actions of the controller or the processor that determines whether or not the processing falls under the territorial scope of the GDPR or not. As such, the processing activities relating to a French citizen living in Canada may or may not fall under applicability of the GDPR depending on who is carrying out the processing activity, but not because the data subject is from France.

2.2 How do the concepts analyzed in the 18 October 2017 memo from Hamilton apply to other domain name-related activities such as escrowing registration data, transferring data to an emergency back-end registry operator in the event of registry failure, and contract enforcement?

2.2.1 If it has been determined that the GDPR is applicable for the processing of personal data carried out by a controller or processor, each different processing activity must be carried out in accordance with the GDPR. As such, controllers and processors must perform a legal analysis of each processing activity in order to make sure that it is GDPR compliant. This legal analysis must take several aspects into account including, but not limited to, the necessity of the processing in regards to their purpose, the personal data used, which legal grounds are applicable, who has access to the data and if the data is transferred to countries outside of the EU or the European Economic Area.

2.2.2 Due to the complexity of determining the legality of a processing activity, it is not possible to determine how the GDPR will affect all domain name-related activities carried out by all parties involved. However, in general the topics analyzed in the October 2017 Memorandum may be necessary to consider with regard to all processing activities.

2.2.3 As regards escrowing of registration data for disaster recovery purposes in particular, we will address this issue further in part 3 of our memoranda series.

2.3 The Article 29 Working Party recently issued revised guidelines on Data Protection Impact Assessments. How do these revised guidelines factor into the recommendation in the 18 October 2017 memo from Hamilton for ICANN to conduct a Data Protection Impact Assessment?

2.3.1 The recommendation and basis for this recommendation to carry out a data protection impact assessments ("**DPIA**") remains unchanged from the analysis in section 3.4.4 of the October 2017 Memorandum after the issuance of the final draft

of the Article 29 Working Party's guidelines on Data Protection Impact Assessment. The final version of the guidelines contains few material changes of when a DPIA is considered necessary.

2.4 Does the GDPR apply retroactively to data processing activities? For example, suppose (1) an EU resident signed a 5-year registration agreement with a registrar for a domain name, (2) the parties are in year two of the 5-year agreement, and (3) the registrar is relying on consent as the legal basis for processing the personal data of the registered name holder. May the registrar wait until the renewal of the registration agreement (i.e. 2020) to obtain consent in the manner required by the GDPR, or must the registrar do so by May 2018?

2.4.1 All processing activities must be based on a legal ground under Article 6.1 GDPR in order to be lawful. Consent is one possible legal ground in Article 6.1(a).

2.4.2 The GDPR will not be applied retroactively to data processing activities already carried out and have since ceased. However, it will apply to data processing activities that are continuously carried out or will be carried out in the future, regardless of when the contract was entered into or when the processing activity commenced. Consequently, any processing of personal data that takes place on 25 May 2018 and afterwards will have to comply with the GDPR.

2.4.3 If consent is the applicable legal ground for the processing activity, it will be necessary to have a valid consent in place as from (and in practice prior to) 25 May 2018. Consents previously collected will still be valid as long as they fulfil the requirements set forth in the GDPR. If the consent was not formulated or collected in a way that is compliant with the GDPR, a new consent must be collected. If no valid consents have been acquired before the GDPR enters into force, the processing will not have a basis in a legal ground, which will constitute an infringement of the GDPR. It should however be noted that the applicable legal ground for each processing activity must be evaluated and a general consent for all processing of personal data is not advised and often not in compliance with the GDPR.

2.4.4 Consequently, if an agreement is in year two of a five-year term and the consent obtained in the agreement is not compliant with the GDPR, a new consent will need to be obtained and in place as from 25 May 2018.

2.4.5 Further information regarding consent is found in section 3.8.2 of the October 2017 Memorandum. As further described therein, our assessment is that the consents that ICANN requires the registrars to obtain under the 2013 Registrar Accreditation Agreement do not fulfil the requirements of the GDPR, as they are likely not to be

deemed freely given, and the registrars will thus not be able to continue to rely on such consents as from 25 May 2018.

2.5 What is the relevance of Article 36 (Prior consultation) and Article 40 (Codes of conduct) to domain name registration data processing and publishing?

2.5.1 Prior consultation with the supervisory authority under Article 36 GDPR is strictly related to the requirement to carry out a data protection impact assessment ("**DPIA**") when a processing activity is likely to present a high risk to the rights and freedoms of the data subjects. If a DPIA is conducted and the risks associated with the processing activities remain high, even after the implementation of measures to mitigate the risks or if no such mitigation actions are performed, a controller must seek consultation from the applicable data protection authority ("**DPA**") regarding the processing activity. The DPA's opinion must be sought before the processing activities commences, unless it concerns processing activities that started before the GDPR comes into effect as in which case prior consultation may be sought as soon as the DPIA is completed. The DPA's opinion may include requirements to perform mitigating actions, prohibition from performing the processing activity or other advice or requests.

2.5.2 In part 3 of our memoranda series, we will elaborate on how a DPIA could potentially be used to seek clarity whether the Whois services could possibly be provided under the GDPR.

2.5.3 Article 40 GDPR encourages the implementation of codes of conduct in order to establish acceptable standards, or best practice standards, for data protection in specific sectors. They are envisioned to guide controllers and processor on how to ensure GDPR compliance within their own business. So far, no codes of conduct have been implemented. Hypothetically, it is possible for a collection of controllers and processors, e.g. registrars, to develop a code of conduct for domain name registration data processing and publishing to be used as a standard for GDPR compliance. Such code of conduct must be submitted to the applicable DPA. Adoption of codes of conduct does not mean that the processing activities performed by a controller or a processor are lawful, each entity must also implement and follow such codes of conduct. They may however, be used to showcase a data protection standard. The GDPR sets out a general procedure for the approval of codes of conduct but does not contain any mandatory possessing times for the DPAs.

2.5.4 Codes of conduct would be a useful tool to provide the gTLD community with common rules to comply with in their processing of personal data. For instance, a

code of conduct could be used to regulate the transfer of personal data to third countries.

2.5.5 While applying an approved code of conduct can be used to demonstrate compliance with the GDPR, it is important to stress that a code of conduct will not change the lawfulness of a processing activity and the implementation of a code of conduct cannot be used to achieve an exemption from the GDPR. Thus, although codes of conduct could be a useful tool for the gTLD community as means for providing registrars and registries with approved guidelines to following, they will not automatically make the processing compliant with the GDPR.

2.6 [FROM GAC COMMUNIQUE – ABU DHABI] What are the options under the GDPR to ensure the lawful availability of WHOIS/RDS data for consumer protection and law enforcement activities? In particular, are there changes to policy or the legal framework that should be considered with a view to preserving the functionality of the WHOIS to the greatest extent possible for these purposes and others also recognized as legitimate? This question includes tasks carried out in the public interest and tasks carried out for a legitimate purpose, including preventing fraud and deceptive activities, investigating and combatting crime, promoting and safeguarding public safety, consumer protection, cyber-security etc.

2.6.1 How to ensure the lawful availability of WHOIS/RDS data will be the primary focus of an upcoming memorandum expected to be published in part 3 of our memoranda series.

2.7 [FROM GAC COMMUNIQUE – ABU DHABI] What are the options under the GDPR to ensure the lawful availability of WHOIS/RDS data for the public, including businesses and other organizations? This question includes tasks carried out in the public interest and tasks carried out for a legitimate purpose, including preventing fraud and deceptive activities, investigating and combatting crime as well as infringement and misuse of intellectual property, promoting and safeguarding public safety, consumer protection, cyber-security etc.

2.7.1 These questions will be further addressed in part 3 of our memoranda series.

2.8 Is there a role for model contract clauses as it relates to the various data processing activities under ICANN policies/contracts and GDPR?

2.8.1 As ICANN, even if it would also be considered to have an establishment in the EU as described in section 2.1.2 above, is considered to be located in a third country (i.e. a country outside of the EU or the European Economic Area) the protection and security of the personal data that is being transferred to ICANN must be

ensured. In accordance with Article 46.2(c) this may be achieved by making the model contract clauses part of the agreement between ICANN and the registrar, see sections 3.3.3 to 3.3.4 of the October 2017 Memorandum for further information regarding model contract clauses.

2.9 ICANN org is working with the community to develop implementation details for consensus policy recommendations governing the accreditation of privacy and proxy providers. How should GDPR requirements be factored into developing the accreditation process?

2.9.1 As with the registration process for registrars, any requirements that ICANN imposes on privacy and proxy providers need to comply with the GDPR. In our assessment, we have not specifically focused on the processing of personal data by such providers but the principles described in our memoranda series will also, as applicable, be relevant for their processing.

2.10 What is the relevance of the "right to object" to the various data processing activities under ICANN policies/contracts?

2.10.1 The right to object under Article 21 GDPR is a right of the data subject to object to processing of his or her personal data in specific circumstances. These circumstances exist if the processing:

(i) is based on public interest, Article 6.1(e) GDPR, as a legal ground;

(ii) is based on public legitimate interest, Article 6.1(f) GDPR, as a legal ground; or

(iii) concerns direct marketing.

2.10.2 The data subject may also object to the use of cookies and similar technology using technical specifications, e.g. settings in the internet browser.

2.10.3 If the data subject has objected to a processing activity object and it concerns direct marketing the processing activities for direct marketing purposes must cease in regards to that data subject. In the other two cases described above the right to object is not absolute and the controller may continue to process the personal data if (i) the controller can demonstrate compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject or (ii) if the processing is necessary for the establishment, exercise and defense of legal claims. Note that it is harder to demonstrate *compelling* legitimate interest in accordance with Article 21 GDPR than using legitimate interests as a legal ground in accordance with Article 6.1(f) GDPR.

2.10.4 In regards to processing activities under ICANN policies and contracts it is primarily in regards to processing under the legal ground of legitimate interest that may primarily be affected by the right to object.

2.11 What is the role of the EU-U.S. Privacy Shield as it relates to the various data processing activities under ICANN policies/contracts and GDPR? What are the eligibility criteria for an organization to participate in the EU-U.S. Privacy Shield? Could ICANN be certified under the Privacy Shield?

2.11.1 As mentioned in section 3.3.6 of the October 2017 Memorandum, transfers from the EU to the United States is permitted if the receiver has been certified under the Privacy Shield framework. There are several criteria an organization must fulfil for joining Privacy Shield, including, but not limited to:

(i) be subject to the investigatory and enforcement powers of U.S. statutory bodies that will ensure compliance with Privacy Shield (currently the Federal Trade Commission and the Department of Transportation);

(ii) implement and disclose privacy policies in accordance with Privacy Shield; and

(iii) publically declare its commitment to adhere to Privacy Shield.

2.11.2 Whether or not ICANN could be certified under the Privacy Shield will require an analysis from a U.S. legal perspective.

2.11.3 It should be noted that Privacy Shield is only relevant with regard to transfers from the EU to the United States and does affect the compliance of the processing as such. Consequently, even if ICANN is certified under Privacy Shield, the underlying processing activities must still comply with the GDPR.

2.12 Please provide additional information concerning Article 49 (Derogations for specific situations) and its applicability to the various data processing activities under ICANN policies/contracts. For example, how do the concepts of "public interest" and "performance of a contract" apply to the processing and publishing of domain name registration data? Could these concepts be used as a justification for continuing to provide open, public access to domain name registration data?

2.12.1 The derogations for specific situations in Article 49 GDPR lists situations where transfer of personal data to a third country are lawful even when the receiving country is not deemed to have adequate protection and no safeguards are in place to ensure the safety of the personal data that is being transferred.

2.12.2 In order for a public interest to exist according to the GDPR, such interest needs to be laid down in either EU law or EU member state national law.

2.12.3 Processing based on performance of a contract is described in section 3.8.3 of the October 2017 Memorandum. As public access is not necessary for the performance of the contract per se, this legal ground cannot be used for such purpose in this context.

2.12.4 It should be noted that several of the specific situations listed in Article 49 GDPR states that the transfer must be necessary for the specific circumstance. As such, it is important to separate the issues whether or not the processing is necessary and whether or not the transfer is necessary. In many cases, even though processing is necessary, e.g. for the performance of a contract, the transfer of the personal data to a third country is not. The latter is true even if the controller, e.g. a registrar, is under contractual obligation to transmit the personal data to ICANN in an agreement between ICANN and the registrar, as it is only the contract between the data subject and the controller that can constitute this necessity. As such, while the processing of domain name registration data could be viewed as necessary for the performance of a contract, in accordance with the legal ground set forth in Article 6.1(b) GDPR, the transfer of the personal data to a third country may not be seen as necessary in accordance with Article 49 GDPR.

2.12.5 Under Article 49 GDPR, it is also possible to collect explicit consent to the transfer in question. The consent must fulfill the obligations set forth in the GDPR, see section 3.8.2 of the October 2017 Memorandum, including that it shall be voluntary and be easy to withdraw. Also, in order for the consent to be valid the data subject must be informed that the transfer is carried out in the absence of safeguards to the protection of the personal data and of the possible risks of the transfer.

2.13 If a contract specifies a legitimate purpose necessary for performing the contract, would a data controller need to obtain explicit consent from the data subject to process personal data?

2.13.1 If the processing is necessary for the performance of a contract between the controller and the data subject or is for the benefit of the data subject, no consent is necessary unless the processing may be deemed high risk or sensitive. For instance, it may be necessary to collect consent if the personal data used include ethnicity or sexuality or if the personal data is transferred to a third country without any safeguards being in place in accordance with Article 49(1) point (a) GDPR.

2.14 How can ICANN registrars, registries, and privacy/proxy providers obtain and document prior consent to transfer registrant data that complies with both GDPR and WHOIS requirements in ICANN policies and agreements?

2.14.1 All controllers and processors must be able to demonstrate that consents were collected and what the data subject consented to, i.e. the content of the consent. In many cases, this will be done by implementing technical solutions that show when a data subject provided his or her consent and how. Also, each version of the consent text should be kept and it should be noted when these consents where in use if it is not possible to save each consent of a data subject in a directory. If the GDPR and the WHOIS requirements in ICANN policies and agreements differ, the consent must either be obtained and documented twice in order to comply with both obligations or, preferably, in a way that complies with both.

2.14.2 How a solution for obtaining and documenting consents may be constructed will depend on the one who collects the consents as no requirements for this is set forth in the GDPR.

2.15 Are there data protection laws in addition to GDPR, and in places other than Europe, that might trigger comparable challenges for ICANN and the domain industry?

2.15.1 There are several EU and national regulations that may affect the processing of personal data, especially in regards to certain sectors and processing carried out for specific purposes. The regulations that primarily affect the domain industry is the EU ePrivacy Directive 2002/58/EC and the proposed new EU ePrivacy Regulation aimed to replace the said directive in May 2018.

2.15.2 Where data is processed outside of the EU (or if non-EU legislation would have extraterritorial reach), other data protection laws than European laws may apply. This is however outside the scope of our assessment and has not been reviewed by us.

2.16 Would a WHOIS model that incorporates the some or all elements outlined below be compatible with GDPR requirements?

(a) Publication of contact data of natural persons in WHOIS by default if natural persons are allowed to opt-out of publication.

(b) Publication of all current WHOIS data if a domain is registered by a natural person not residing in the European Union.

(c) Publication of all current WHOIS data if a domain is registered by a legal person.

(d) Publication of "thin" WHOIS data for all domain registrations (e.g. nameservers, domain name expiration date, sponsoring registrar, etc.)

(e) Publication of all contact data (e.g. name, email address, mailing address, telephone number, etc.) for administrative and technical contacts in WHOIS for all domain name registrations.

(f) Transfer from registrar to registry of all current registration data required by ICANN policies and agreements (whether or not the information is ultimately published in WHOIS services).

2.16.1 These questions will be further addressed in part 3 of our memoranda series.

2.17 Are IP addresses considered personal data under the GDPR?

2.17.1 Whether or not IP addresses are considered personal data under the GDPR have been under some debate. An IP-address is considered personal data if it can be connected to a natural person. This has meant that in general, static IP addresses are considered personal data whereas dynamic IP addresses may be considered personal data. Some DPA's, such as the Swedish DPA (Sw. "*Datainspektionen*"), have previously interpreted the term personal data broadly in this context. This has resulted in that the Swedish DPA seems to consider all IP addresses as personal data as it is, at least theoretically, possible to link the IP address to a natural person, even if this is very difficult and require the cooperation of the telecommunications service provider. This view is supported by the ruling of the Court of Justice of the EU (the "CJEU") in Case 582/14, where it is stated that the fact that the additional data necessary to identify a website user is held by that user's internet service provider does not appear to be such as to exclude that dynamic IP addresses constitute personal data.

2.17.2 Given the above views by the CJEU and certain DPAs, we recommend taking the principal approach that, as regards Whois data, dynamic IP addresses are to be considered to be personal data.

2.18 Would a domain name that consists of the first and last name of a natural person be considered personal data under the GDPR? Also, for GDPR compliance, could

a different approach be taken for handling data on registrants who are individuals versus those who are organizations?

2.18.1 All domain names could constitute personal data if it can be linked to a natural person. If a domain name consists of the first and last name of a natural person it would be personal data as it adheres to a natural person even if it is not obvious exactly which person it is, e.g. if the name in question is very common.

2.18.2 Information regarding legal persons is generally not personal data. However, in some cases the connection between the organization and one natural person is especially strong, e.g. when it is a sole trader. In these cases, the information regarding the legal person could be considered personal data and an analysis would have to be carried out in each case. Also, information that adheres to the employees of the organization is considered personal data. Therefore, it is in theoretically possible to have a different approach to natural persons and organizations but, considering the legal analysis that would have to be performed in each case, such an approach may be practically inefficient.

2.19 [FROM ICANN INTELLECTUAL PROPERTY CONSTITUENCY] ("IPC") How can the current WHOIS protocol be maintained to the greatest extent possible while still not violating GDPR, recognizing the strong public policy justifications for having WHOIS data quickly and easily accessible for the purposes set forth in the GAC advice dated Nov. 1, 2017? Can Hamilton further analyze the viability for public disclosure and/or access to WHOIS/RDS data in compliance with GDPR in light of the recent CJEU decision in the issue of Manni (2017), and consideration of WHOIS/RDS data as a form of a public ownership record for domains?

2.19.1 This will be further addressed in part 3 of our memoranda series.

2.20 [FROM IPC] Could ICANN and/or contracted parties, in their capacities as controllers, invoke the prior consultation provisions of Article 36 of the GDPR to gain greater clarity about the compatibility of either current or proposed modified WHOIS practices with the requirements of GDPR, by obtaining the "written advice" of a member state data protection authority? If so, what are the pro's and con's of doing so?

2.20.1 This will be further addressed in part 3 of our memoranda series.

2.21 [From IPC] Does Article 40 provide a reasonable basis for ICANN and/or the domain name industry generally, to establish a GDPR compliant system for collection and transmission of data of natural persons in accordance with legitimate interests? If so, what advice does Hamilton have in connection with

the preparation of a draft Article 40 submission (i.e. what is the procedure, what are the time lines to obtain advice prior to implementation of GDPR, etc.)? Could such a submission be made in advance of May 2018 to the Article 29 Working Group, whose opinion could later be adopted by the EDPB?

2.21.1 Please see our answer in section 2.5 above with regard to codes of conduct. While codes of conduct surely can be a useful instruments in terms of providing registrars and registries with a common collection of rules to adhere to, it will not solve the issue of whether the processing of personal data within the scope of the Whois services is lawful under the GDPR or not. In part 3 of our memoranda series, we will further discuss how a GDPR compliant system could be constructed.

2.22 [FROM IPC] How and under what circumstances can contractual performance be grounds for justifying collection, use and provision of access to personal data in the WHOIS/RDS? Is the fact that ICANN and the registry may be considered joint controllers relevant to the inquiry of whether the agreement with the registrant is independent of the registrar's agreement with ICANN? Is the fact that registrars and/or registries are obliged to adhere to WHOIS obligations pursuant to ICANN policy relevant to this inquiry? How does the availability of privacy/proxy services affect this analysis?

2.22.1 Contractual performance can only constitute legal ground for processing where the controller has a contract directly with the data subject. Thus, registrars should be able to rely of performance of contract as legal ground for purposes that are necessary for performing the contract, but this ground cannot be used for processing by ICANN or registries. This will be further addressed in part 3 of our memoranda series.

2.23 [FROM IPC] In paragraph 3.8.5.1, the Hamilton memorandum opines "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." Could Hamilton expand on its view of what changes to current WHOIS policies would be minimally required to change this conclusion? Does the recent GAC advice on WHOIS change this analysis? Can Hamilton provide a deeper analysis of the balancing test required under the legitimate interests prong for processing, taking into account the recent CJEU decision in the issue of Manni (2017)?

2.23.1 This will be further addressed in part 3 of our memoranda series.

2.24 [FROM IPC] The Hamilton memo does not discuss Art. 6(1)(e) of GDPR as a possible basis for processing of registration data. This provision addresses

"processing [that] is necessary for the performance of a task carried out in the public interest….". In view of the longstanding role of WHOIS data in advancing consumer protection, buttressing the rule of law online, and facilitating the ability of Internet users to know with whom they are dealing online, and in light of ICANN's over-arching responsibility to act in the public interest, could Hamilton analyze the extent to which Art. 6(1)(e) may provide a basis for processing of registration data? Is this a sufficient basis for a publically accessible WHOIS? If not, why not, and what type of access / disclosure / processing would be possible under this public interest prong?

2.24.1 See section 2.12.2 above. Public interest in accordance with Article 6.1(e) GDPR essentially only exists where such interest is codified under law, and ICANN may not rely on this legal ground for processing of Whois data. Public interest as legal ground for processing will be further discussed in part 3 of our memoranda series.

2.25 [FROM ICANN BUSINESS CONSTITUENCY ("BC")] Section 3.2.1 of the October 2017 Memorandum states the following: "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.".

Are companies that offer services only to organizations and not to individuals excepted from (a) above, since the service is not given to a 'data subject' who by definition of GDPR is a natural person?

2.25.1 Yes, given that these would be the actual circumstances, our opinion is that that would be the case.

2.26 [FROM BC] Is behavior online necessarily behavior in the EU? Example: If an individual in Germany changes the IP address of his/her domain name, and that IP address is not hosted in the EU, is that considered 'behavior that takes place in the EU"? Can this be clarified, please?

2.26.1 We have not assessed this question in closer detail at this stage. In our opinion, Article 3.2(a) GDPR ("the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union") is applicable, which is sufficient.

2.27 [FROM BC] Are the purposes listed in section 3.8.4.3(i)-iv) of the October 2017 Memorandum considered "legitimate interests" under Article 6.1(f) GDPR?

2.27.1 While the purposes listed could surely constitute legitimate interest (basically any lawful interest could), the question is whether they could be considered to override the the fundamental rights and freedoms of the data subject, which is required in order for such interest to constitute legal ground in accordance with Article 6.1(f) GDPR. This will be further addressed in part 3 of our memoranda series.

2.28 [FROM BC] Would item (ii) section 3.8.4.3 of the October 2017 Memorandum apply only to matters that are a "violation of law"? That is, is it a legitimate use of Whois to prevent consumer deception with the understanding that not all consumer deception may have an applicable law against it?

2.28.1 This will be further addressed in part 3 of our memoranda series. It should be noted that section 3.8.4.3 of the October 2017 Memorandum is not intended to be exhaustive but rather to be illustrative examples of purposes that could constitute legitimate interest.

2.29 [FROM BC] How can ICANN assure that essential access to Whois will enable the legitimate interests described above?

2.29.1 This will be further addressed in part 3 of our memoranda series.

2.30 [FROM BC] Can a Code of Conduct be developed by ICANN to apply to WHOIS? Please describe the pros/cons of using a Code of Conduct approach? Are there any industries or companies contemplating a code of conduct approach or have taken steps to put together a Code of Conduct?

2.30.1 Please see our answer in sections 2.5 and 2.21.1 above with regard to codes of conduct. Within the scope of our assessment, we have not looked into whether any industries or companies are contemplating a code of conduct approach.

2.31 [FROM BC] How can ICANN seek a public interest exemption, and under what circumstances have such an exemption been recognized? Is there any guidance on what is meant by the "public interest"? How are real estate ownership records or corporate registration registers able to comply with GDPR? (See for example, the CJEU's 2017 decision in Manni, involving the corporate insolvency records posted in a publicly available Italian register).

2.31.1 See sections 2.12.2 and 2.24.1 above regarding public interest in general. It is not possible to seek "public interest exemption" *per se*. Public interest, as well as the

Manni case, and the relation between public interest and legitimate interest will be further addressed in part 3 of our memoranda series.

2.32 [FROM BC] EU law requires public WHOIS for domain names (ccTLDs) – recognizing the public interest served by having this information publicly available. Is there any case law or opinion that would indicate that the rationale for these laws would not also be applicable to gTLDs? (See the Finnish Domain Name Act and European Commission regulations No. 733/2002 and No. 874/2004).

2.32.1 These laws as such are not applicable to gTLDs. When assessing the balancing of interests in accordance with Article 6.1(f) GDPR, such laws can however be used as argument for the existence of sufficient legitimate interest. This will be further addressed in part 3 of our memoranda series.

2.32.2 It should be noted that the Finnish Domain Name Act referred to in the question, which contained a requirement mandatory publication of registration data regarding .fi ccTLDs with an opt-out option for natural persons except with regard to the domain name and the registrant's name, which was always mandatory information, has been revoked and replaced by the Finnish Information Society Code. The Finnish Information Society Code contains less strict publication requirements, stating that the authority managing the Finnish domain name register for .fi ccTLDS *may* disclose information from the domain name register, and that information regarding registrants which are natural persons shall be limited to the domain name and the name of the registrant.

2.33 [FROM BC] Are there any cases where provisions of industry-wide agreements have been challenged for failing to comply with the EU privacy laws? Is there any guidance on how to interpret "necessary for the performance of a contract"?

2.33.1 Within the scope of our assessment, we have at this stage not looked into whether there are any such cases.

2.33.2 The interpretation of "necessary for the performance of a contract" is rather clear. As has been addressed in the October 2017 Memorandum and above in this memorandum, this legal ground can only be applied where the controller is a party to a contract and needs to process data for the relevant purpose in order to fulfil its obligations under such contract.

2.34 [FROM ISPCP CONSTITUENCY] Whois output has been the subject of a lot of discussion and analysis. Are there any plans to provide a legal assessment of the data elements that can be collected in the first place?

2.34.1 This will be further addressed in part 3 of our memoranda series.

2.35 [FROM ISPCP CONSTITUENCY] Will there be any analysis of the retention periods for data elements, i.e. when individual data elements need to be deleted or blocked?

2.35.1 Within the scope of our assignment, we have not addressed this issue in detail. While this is an important question, our assignment has focused on whether Whois data can be processed within the scope of Whois services in the first place. When a model for processing of Whois data has been determined, the question of retention periods is of course important, but has not been the focus of our assessment at this stage.

2.35.2 In short, personal data shall not be stored for longer than is necessary for the purposes of which the data is processed (Article 5.1(e) GDPR). For Whois services, that would most likely mean that personal data, as a general rule, must be deleted when the domain name registration in question ceases, unless the data for some reason is needed for a longer period for a specific purpose (for instance complete the invoicing). It may however then only continue to be processed for that purpose and not for any other purpose.