DRAFT Questions for GDPR Legal Analysis (Part 2) and Additional Background Resources

As of 15 November 2017

ICANN has engaged 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 being conducted in iterative phases, and the following questions have been gathered from discussions and submissions from the community to provide as consideration and for possible discussion in Part 2 of the analysis.

Draft Questions for GDPR Legal Analysis (Part 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. 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?
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?
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?
5. What is the relevance of Article 36 (Prior consultation) and Article 40 (Codes of conduct) to domain name registration data processing and publishing?
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.

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.
8. Is there a role for model contract clauses as it relates to the various data processing activities under ICANN policies/contracts and GDPR?
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?
10. What is the relevance of the "right to object" to the various data processing activities under ICANN policies/contracts?
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?
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?
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?
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?
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?
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).

17. Are IP addresses considered personal data under the GDPR?
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?

Additional Resources

- 9 October 2017 letter from Jetse Sprey to Göran Marby re: Gemeente Amsterdam FRL Registry B.V. https://www.icann.org/en/system/files/correspondence/sprey-to-Marby-9oct17-en.pdf
- 10 October 2017 letter from Jean-Jacques Sahel to Elena Plexida (European Commission, CONNECT Directorate General) re: request for information as part of our fact-finding exercise on GDPR https://www.icann.org/en/system/files/correspondence/sahel-to-plexida-10oct17-en.pdf
- 24 October 2017 Memorandum from Taylor Wessing law firm commissioned by the ICANN Intellectual Property Constituency regarding the impact of the GDPR on the Whois system: https://www.icann.org/en/system/files/correspondence/sheckler-to-swinehart-atallah-29oct17-en.pdf.
- 2 November 2017 ICANN Contractual Compliance Statement re: Impact of GDPR on enforcement of WHOIS and other contractual requirements related to domain name registration data: https://www.icann.org/resources/pages/contractual-compliance-statement-2017-11-02-en.
- 29 October 2017 letter from Elena Plexida (European Commission, CONNECT Directorate General) re: Information on WHOIS policies implemented for the .eu TLD https://www.icann.org/en/system/files/correspondence/plexida-to-sahel-29oct17-en.pdf
- 1 November 2017 GAC Communiqué – Abu Dhabi https://www.icann.org/en/system/files/correspondence/gac-to-icann-01nov17-en.pdf

- 1 November 2017 Letter from John O. Jeffrey to Jetse Sprey re: Gemeente Amsterdam FRL Registry B.V. https://www.icann.org/en/system/files/correspondence/jeffrey-to-sprey-01nov17-en.pdf

ICANN | IPC
Intellectual Property Constituency

November 14, 2017

To: Göran Marby, Chief Executive Officer
Theresa Swinehart, SVP Multistakeholder Strategy Initiatives
Akram Atallah, President Global Domains Division

Re: Impact of the General Data Protection Regulation on the WHOIS system – Additional Questions for Hamilton

Dear Göran, Theresa and Akram,

Pursuant to Göran's invitation in Abu Dhabi, we would appreciate it if ICANN would ask the following GDPR/WHOIS related questions to Hamilton:

General:

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?

Prior Consultation (Article 36)

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?

Code of Conduct (Article 40)

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?

Use/Disclosure For Contractual Performance (Article 6(1)(b):

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?

Use/Disclosure For Legitimate Interests (Article 6(1)(f):

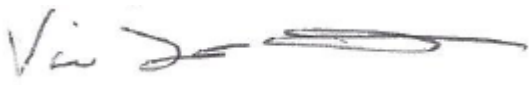
In paragraph 3.8.5.1, the Hamilton memorandum opines "it will not be possible to claim legitimate interest as a legal ground for processing of personal data as currently performed through the WHOIS services on an unchanged basis." Could Hamilton expand on its view of what changes to current WHOIS policies 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)?

Use/Disclosure For Public Interest (Article 6.1(e):

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?

Thank you for the opportunity to raise these additional questions, and we look forward to receiving Hamilton's advice on these issues. If you have any concerns or comments about our questions, please don't hesitate to contact me.

Regards,



Vicky Sheckler

Vice President, Intellectual Property Constituency

ICANN Business Constituency (BC) Questions for Hamilton's legal analysis of GDPR and Whois

14-Nov-2017

Regarding Section 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".

Question 1: 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?

Question 2: 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?

Regarding Section 3.8.4.3: Looking at the current Whois services, there are several uses that could qualify as legitimate interests. For instance, recital 47 GDPR specifically mentions processing necessary for preventing fraud as a legitimate interest. And the Article 29 Working Party indicated that the "combatting of file sharing" could constitute a legitimate interest. So 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 criminal behavior which could include: child online exploitation; phishing scams that exploit individual users; other forms of online fraud, consumer deception, abuse of trademarks or other
> 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 and to allow a consumer to validate the authenticity of the offering company.
>
> (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.

Question 3: Are the purposes above considered "legitimate interests" under Article 6.1(f) GDPR?

Question 4: Would item (ii) above 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?

In its Bylaws, ICANN acknowledges its commitment to "(i) Preserve and enhance the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and

openness of the DNS and the Internet". Whois is critical to enabling those who combat fraud and abuse of domain names.

Question 5: How can ICANN assure that essential access to Whois will enable the legitimate interests described above?

Question 6: 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?

Question 7: 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).

Question 8: 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.

A public WHOIS database is necessary for the performance of a contract - it is a requirement placed by ICANN for the registration agreements between registrants and registrars, as well as under the RAA and the Registry Agreements. ICANN's bylaws mandate a periodic review of Registration Directory Service, 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."

Question 9: 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"?

From: "Wolf-Ulrich.Knoben"
Date: Tuesday, November 14, 2017 at 10:10 AM
To: "gdpr@icann.org" <gdpr@icann.org>
Cc: Rickert Thomas , Steffen Lars
Subject: [Ext] FOR REPLY BY 10-Nov: we need GDPR questions for the Hamilton law firm

Hi Teresa and Akram,

we would like to provide the following two questions:

1. 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. Will there be any analysis of the retention periods for data elements, i.e. when individual data elements need to be deleted or blocked?

Thanks and best regards
Wolf-Ulrich Knoben
Chairman ISPCP Constituency