

ANLAGE

AG 5



Brussels, 5 July 2018
EDPB-85-2018

Mr Göran Marby
President and CEO of the Board of Directors
Internet Corporation for Assigned Names and Numbers (ICANN)
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536

Dear Mr. Marby,

I am writing you in response to your letter of 10 May 2018. In your letter you raise a number of questions, many of which have already been the topic of discussion during the meeting between ICANN and WP29 Members on 23 April 2018.

On 25 May 2018, the European Data Protection Board (EDPB) endorsed the WP29 statement regarding WHOIS.¹ The statement confirms the expectation of the EDPB towards ICANN to develop a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data.

The EDPB has also taken note of the Temporary Specification adopted by ICANN on 17 May 2018, in which the ICANN Board establishes temporary requirements, effective as of 25 May 2018, which seek to allow ICANN and gTLD registry operators and registrars to continue to comply with existing ICANN contractual requirements and community-developed policies in light of the GDPR.²

Given the interim adoption of the Temporary Specification, the EDPB will respond to the questions raised by your letter in relation to those issues requiring immediate further consideration as ICANN proceeds to develop a GDPR-complaint WHOIS model. Needless to say, the issues identified here are without prejudice to additional issues, further inquiries or findings being made by the EDPB or its Members at a later date.

¹ https://edpb.europa.eu/news/news/2018/european-data-protection-board-endorsed-statement-wp29-icannwhois_it

² <https://www.icann.org/en/system/files/files/gtld-registration-data-temp-spec-17may18-en.pdf>

1. Purpose specification and lawfulness of processing

In its letter of 11 April 2018, WP29 stressed the importance of explicitly defining legitimate purposes in a way which comports with the requirements of the GDPR.³ In its letter of 10 May 2018, ICANN makes several references to ICANN's Bylaws to underline that ICANN's mission with respect to domain names is not limited to ensuring the stable and secure operation of the Internet's unique identifier system (technical stability).

The EDPB has taken note of ICANN's Bylaws, which require ICANN, in carrying out its mandate, and in particular as part of its review processes, 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"⁴ and to "adequately address issues of competition, consumer protection, security, stability and resiliency, malicious abuse issues, sovereignty concerns and rights protection"¹ prior to authorizing an increase in the number of gTLDs in the root zone.⁵

Nevertheless, the EDPB considers it essential that a clear distinction be maintained between the different processing activities that take place in the context of WHOIS and the respective purposes pursued by the various stakeholders involved. There are processing activities determined by ICANN, for which ICANN, as well as the registrars and registries, require their own legal basis and purpose, and then there are processing activities determined by third parties, which require their own legal basis and purpose.

The EDPB therefore reiterates that ICANN should take care not to conflate its own purposes with the interests of third parties, nor with the lawful grounds of processing which may be applicable in a particular case.

A clear definition of the specific purposes pursued by ICANN (and registrars and registries) at the moment of collection would not categorically exclude the subsequent disclosure of personal data to third parties for their own (legitimate) interests and purposes, provided the requirements of the GDPR are met.⁶ Article 6(1)f GDPR provides a legal basis for controllers to disclose personal data for the purposes of the legitimate interests third parties, provided that those interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data.⁷ Indeed, recital (47) of the GDPR provides that

"The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data

³ Article 29 Working Party, Letter to Mr. Göran Marby of 11 April 2018, p. 3.

⁴ ICANN Bylaws Section 4.6(e)(ii), available at <https://www.icann.org/resources/pages/governance/bylaws-en>.

⁵ ICANN Bylaws Section 4.6 (d).

⁶ See for example the CJEU judgment in *Rigas* (C-13/16), concerning the disclosure of personal data necessary in order to exercise a legal claim.

⁷ Depending on the circumstances, the disclosure may also be justified pursuant another lawful basis, such as compliance with a legal obligation to which the controller is subject (article 6(1)c).

subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.”

As a result, the personal data processed in the context of WHOIS can be made available to third parties who have a legitimate interest in having access to the data, provided that appropriate safeguards are in place to ensure that the disclosure is proportionate and limited to that which is necessary and the other requirements of the GDPR are met, including the provision of clear information to data subjects.

2. Collection of “full WHOIS data”

In its letter of 10 May 2018, ICANN asks whether the collection of “full WHOIS data” from registrants by the registrar activities is considered to be excessive in relation to the purposes pursued.

In terms of the information collected, ICANN currently requires registrars to collect, among others, contact details about the registrant, including names, phone (and where available fax) number, postal address, and email addresses.⁸ It requires the similar contact details to be collected in relation to the administrative and technical contacts associated with the domain name registration.⁹

On 25 May 2018, ICANN initiated legal proceedings against a registrar who announced that it would no longer collect information on the technical and administrative contacts associated with a particular domain name registration.¹⁰ On 30 May 2018, the Regional Court of Bonn, denied ICANN’s request for injunctive relief, on the basis that

“The Applicant has not demonstrated that the storage of other personal data than that of the domain holder, which continues to be indisputably collected and stored, is indispensable for the purposes of the Applicant. It is obvious that more data makes the identification of persons behind a domain and contacting them appear more reliable than if only one data record of the person generally responsible for the domain is known. However, the domain name holder registered or to be registered is the person responsible for the contents of the relevant website, who does not necessarily have to be different from

⁸ Additional data elements include: registered name, information about the primary and secondary name server(s) for the registered name, information about the registrar, and the original creation and expiration dates of the registration. See section 3.3.1.1-8 of the 2013 Registrar Accreditation Agreement, available at <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>. See also ICANN, Interim Model for Compliance with ICANN Agreements and Policies in relation to the European Union’s General Data Protection Regulation – Working Draft for Continued Discussion” published on 8 March 2018, p. 9 and p. 42-45, available at <https://www.icann.org/en/system/files/files/edpr-compliance-interim-model-08mar18-en.pdf>.

⁹ Idem.

¹⁰ ICANN, English translation of Motion for the issuance of a preliminary injunction, *ICANN v. EPAG Domain services, GmbH*, 25 May 2018, available at <https://www.icann.org/en/system/files/files/litigation-icann-v-epag-request-prelim-injunction-redacted-25may18-en.pdf>

the Tech-C and Admin-C categories, in other words, can combine all those functions on itself.”¹¹

ICANN has appealed the decision on 13 June 2018.¹² In its motion for appeal, ICANN further clarifies that it is not an obligation for registrars to require registrants to name an administrative or technical contact person different to the registrant.¹³ In other words, the contact information for the administrative and technical contacts can be the same as the contact details of the registrant itself. ICANN also clarifies that the administrative or contact person may be a legal person and that it is not necessary that the contact information provided directly identifies a natural person.¹⁴

The EDPB considers that registrants should in principle not be required to provide personal data directly identifying individual employees (or third parties) fulfilling the administrative or technical functions on behalf of the registrant. Instead, registrants should be provided with the option of providing contact details for persons other than themselves if they wish to delegate these functions and facilitate direct communication with the persons concerned. It should therefore be made clear, as part of the registration process, that the registrant is free to (1) designate the same person as the registrant (or its representative) as the administrative or technical contact; or (2) provide contact information which does not directly identify the administrative or technical contact person concerned (e.g. admin@company.com). For the avoidance of doubt, the EDPB recommends explicitly clarifying this within future updates of the Temporary Specification.¹⁵

3. Registration of legal persons

In its letter of 10 May 2018, ICANN asks whether the proposed interim compliance model should apply to domain name registrations that include personal data associated with a registration of a legal person.

The GDPR does not apply to the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.¹⁶ While the contact details of a legal person are outside the scope of the GDPR, the contact details concerning natural persons are within the scope of the GDPR, as well as any other information relating to an identified or identifiable natural person.¹⁷

¹¹ ICANN, English translation English of Court Order on Application for Preliminary Injunction, *ICANN v. EPAG Domainservices, GmbH*, 30 May 2018, available at <https://www.icann.org/en/system/files/files/litigation-icann-v-epag-request-court-order-prelim-injunction-redacted-30may18-en.pdf>.

¹² <https://www.icann.org/en/system/files/files/litigation-icann-v-epag-immediate-appeal-redacted-13jun18-en.pdf>.

¹³ ICANN, English translation of Immediate Appeal, *ICANN v. EPAG Domainservices, GmbH*, 13 June 2018, p. 6, available at <https://www.icann.org/en/system/files/files/litigation-icann-v-epag-immediate-appeal-redacted-13jun18-en.pdf>.

¹⁴ ICANN, English translation of Immediate Appeal, *ICANN v. EPAG Domainservices, GmbH*, 13 June 2018, p. 18.

¹⁵ The notice requirements applicable to registrars described in the Temporary Specification (in particular at paragraph 7.1.3) do not clearly state that the provision of separate administrative and technical contact details is voluntary rather than obligatory. Moreover, it should be ensured that the individual concerned is informed. See also article 26 GDPR concerning joint controllers.

¹⁶ Recital (14) GDPR.

¹⁷ Article 4(1) GDPR.

The mere fact that a registrant is a legal person does not necessarily justify unlimited publication of personal data relating to natural persons who work for or represent that organization, such as natural persons who manage administrative or technical issues on behalf of the registrant.

For example, the publication of the personal email address of a technical contact person consisting of firstname.lastname@company.com can reveal information regarding their current employer as well as their role within the organization. Together with the address of the registrant, it may also reveal information about his or her place of work.

In light of these considerations, the EDPB considers that personal data identifying individual employees (or third parties) acting on behalf of the registrant should not be made publically available by default in the context of WHOIS. If the registrant provides (or the registrar ensures) generic contact email information (e.g. admin@domain.com), the EDPB does not consider that the publication of such data in the context of WHOIS would be unlawful as such.

4. Logging of access to non-public WHOIS data

In its letter of 11 April 2018, WP29 indicated that *"ICANN should ensure that registrars and registries have appropriate logging and auditing mechanisms in place to detect possible misuse. Such logging mechanisms may also be necessary to ensure individuals can exercise their rights, in particular their right of access."*¹⁸

In its letter of 10 May 2018, ICANN raises the following questions:

- a. Must the identity of the person/entity submitting a WHOIS query be required to be visible to the registrant or other third parties? If so, would this apply to all queries of a registry's or registrar's WHOIS database, including queries of data published in public WHOIS?
- b. Must requests from law enforcement for access to non-public WHOIS be required to be visible to the registrant or other third parties?

The EDPB considers that, unless there is an explicit prohibition in national law, appropriate logging mechanisms should be in place to log any access to non-public personal data processed in the context of WHOIS. In this context, such logging is considered required as part of the security obligation of controllers (article 32), as well as the obligation and in order to be able to demonstrate compliance with the GDPR (accountability) (article 5(2)).

Ensuring traceability of access through appropriate logging mechanisms does not necessarily require active communication (pushing) of log information to the registrant or third parties. It is up to ICANN and other controllers participating in the WHOIS system to ensure that logging information is not disclosed to unauthorized entities, in particular with a view of not jeopardizing legitimate law enforcement activities. Data subject rights, including the right of access, must however be accommodated unless one of the exceptions under the GDPR applies or if national legislation provides for a restriction in accordance with the GDPR (article 23).

¹⁸ Article 29 Working Party, Letter to Mr. Göran Marby of 11 April 2018, p. 5-6.

5. Data retention

In its letter of 10 May 2018, ICANN asks whether the WP29 has a view of the appropriate data retention period that should be considered. As previously indicated by the WP29 in its letter of 11 April 2018, personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (article 5(2) GDPR). This is a matter which has already been addressed repeatedly by both the WP29 and the EDPB.¹⁹ It is for ICANN to determine the appropriate retention period, and it must be able to demonstrate why it is necessary to keep personal data for that period. So far ICANN is yet to demonstrate why each of the personal data elements processed in the context of WHOIS must in fact be retained for a period of 2 years beyond the life of the domain name registration. The EDPB therefore reiterates the request ICANN to re-evaluate the proposed retention period of two years and to explicitly justify and document why it is necessary to retain personal data for this period in light of the purposes pursued.

6. Codes of conduct and accreditation

In its letter of 10 May 2018, ICANN asks whether codes of conduct or accreditation/certification envisaged by article 41-43 are available to ICANN and the Domain Name System (DNS) community as a framework for developing a program for those with a legitimate interest to access non-public WHOIS data.

In this respect, the EDPB wishes to underline first and foremost that codes of conduct, certification and/or accreditation are voluntary measures, which controllers or other representative bodies may develop with a view of helping to demonstrate compliance with the provisions of the GDPR. Putting in place such measures is therefore not required by the GDPR. In addition, plans to develop or adopt such measures in the future cannot serve to delay or replace compliance with controller obligations.

ICANN and the registrars/registries are, as controllers, responsible for ensuring that personal data processed in the context of WHOIS are only disclosed to third parties with a legitimate interest or other lawful basis under the GDPR, also taking into account the other requirements of the GDPR. This implies putting in place an appropriate access model, with appropriate safeguards, including measures to ensure a sufficient degree of compliance assurance. The responsibility for designing a model that will provide this assurance is in first instance up to ICANN and the registrars/registries.

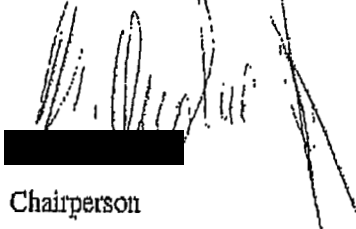
¹⁹ See e.g. Article 29 Working Party, Letter to Dr. Stoye Crocker and Mr. Akram Atallah, 26 September 2012; Article 29 Working Party, Letter to Mr. John. O Jeffrey, 8 January 2014 and European Data Protection Supervisor, Letter to Mr. John. O. Jeffrey, 17 April 2014.

If ICANN decides to pursue the development of codes of conduct, certification and/or accreditation mechanisms in accordance with the GDPR, it must ensure that all the relevant provisions of the corresponding GDPR articles shall be complied with. ICANN should therefore carefully consider how all the requirements included in Chapter IV GDPR for Codes of Conduct and Accreditation shall be met to ensure that the envisaged mechanisms are fully compatible with the GDPR. As far as accreditation is concerned, the EDPB refers to the draft guidelines developed by the WP29,²⁰

The EDPB is confident that the guidance contained in this letter, in combination with the guidance previously issued by the WP29, will enable ICANN to develop a GDPR-compliant model for access to personal data processed in the context of WHOIS.

Sincerely,

On behalf of the EDPB



Chairperson

²⁰ See Article 29 Working Party, Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679, WP261, 6 February 2018.