ARTICLE 29 Data Protection Working Party

Brussels, 11 April 2018

Mr Göran Marby
President and CEO of the Board of Directors
Internet Corporation for Assigned Names and Numbers (ICANN)

Dear Mr Marby,

I refer to your letter of 15 January 2018, in which you outline the steps being undertaken by ICANN to ensure that WHOIS directories and services will be compliant with the GDPR.

The WP29 has taken note of these steps, in particular of the public review of three proposed models for altering WHOIS services launched on 12 January 2018[1]. It has also taken note of the more recent publications of "the Proposed Interim Model for GDPR Compliance – Summary Description" published on 28 February 2018 (hereafter: "Proposed Interim Model")[2] and of the "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 (hereafter: "Final Interim Model")[3].

The WP29 welcomes the fact that ICANN continues to make progress towards GDPR compliance with respect to the WHOIS directories and services. In particular, it welcomes the decision of ICANN to propose an interim model which involves layered access, as well as an "accreditation program" for access to non-public WHOIS data. The WP29 also welcomes the proposal to introduce alternative methods to contact registrants or administrative and technical contacts, without public disclosure of registrants' personal email addresses (referred to as "anonymized email, web form, or other technical means").

The WP29 continues to have concerns, however, regarding several aspects of the Proposed and Final Interim Model. Attached to this letter you will find the areas for which the WP29 considers it of utmost importance that ICANN either reconsider or further evaluate its current approach. The concerns highlighted here are without prejudice to additional concerns, further inquiries or findings being made by the WP29 or its members at a later date.

The WP29 will continue to monitor ICANN's progress closely and its members may, at an appropriate time, engage further with ICANN directly on these issues. In this regard, the WP29 refers also to the Working Paper on Privacy and Data Protection Issues with Regard to Registrant data and the WHOIS Directory at ICANN, adopted by the International Working Group on Data Protection in Telecommunications ("Berlin Group")[4]. While this Working Paper does not reflect the official viewpoint of the Article 29 Working Party, several of its members have actively contributed to the drafting of this paper. As such, the WP29 encourages ICANN take careful consideration of the recommendations outlined in this paper

[1] https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf
[2] https://www.icann.org/news/blog/data-protection-privacy-update-seeking-input-on-proposed-interim-model-for-gdpr-compliance
[3] https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf
[4] Available at https://www.datenschutz-berlin.de/working-paper.html

going forward. WP29 would highlight the importance of ICANN communicating its full plan and timescale by which the solutions will be implemented.

Sincerely,

On behalf of the Article 29 Working Party

Andrea Jelinek

Chairperson

ANNEX

Purpose specification

The WP29 considers that not all of the purposes set forth in the Final Interim Model meet the requirements of article 5(1)b GDPR. The Final Interim Model provides as follows:

> "*For these reasons, it is desirable to have a WHOIS system, the purposes of which include:*
>
> *a. Providing legitimate access to accurate, reliable, and uniform registration data;*
>
> *b. Enabling a reliable mechanism for identifying and contacting the registrant;*
>
> *c. Enabling the publication of technical and administrative points of contact administering the domain names at the request of the registrant;*
>
> *d. Providing reasonably accurate and up to date information about the technical and administrative points of contact administering the domain names;*
>
> *e. Supporting a framework to address issues involving domain name registrations, including but not limited to: consumer protection, investigation of cybercrime, DNS abuse, and intellectual property protection; and*
>
> *f. Providing a framework to address appropriate law enforcement needs;*
>
> *g. Facilitating the provision of zone files of gTLDs to Internet users;*
>
> *h. Providing mechanisms for safeguarding registrants' registration data in the event of a business or technical failure, or other unavailability of a registrar or registry;*
>
> *i. Coordinating dispute resolution services for certain disputes concerning domain names;*
>
> *j. Handling contractual compliance complaints submitted by registries, registrars, registrants, and other Internet users"* [5].

Article 5(1)b GDPR provides inter alia that personal data shall be "collected for specified, explicit and legitimate purposes". In its Opinion on purpose limitation, the WP29 has clarified that purposes specified by the controller must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied.[6] Not all of the purposes enumerated in the Final Interim Model satisfy these requirements. Providing "legitimate access" to "accurate, reliable and uniform registration data", for example, does not amount to a specified purpose within the meaning of article 5(1)b GDPR, as it does not allow to determine what kind of processing is or is not included, nor does it enable a subsequent assessment of compliance or compatibility in case access is provided.

The WP29 stresses the importance of explicitly defining legitimate purposes in a way which comports with the requirements of the GDPR. It therefore urges ICANN to revisit its current definition of "purposes" in light of these requirements. Moreover, it notes that the purposes must be defined in a comprehensive and exhaustive manner. Use of the word "include" suggests that not all purposes are made explicit, which would also be incompatible with

[5] Section 7.2.1 of the Final Interim Model
[6] Opinion 03/2013 on purpose limitation, WP 203, 2 April 2013, p. 15.

article 5(1)b GDPR. Finally, ICANN should take care in defining purposes in a manner which corresponds to its own organisational mission and mandate, which is to coordinate the stable operation of the Internet's unique identifier systems. Purposes pursued by other interested third parties should not determine the purposes pursued by ICANN. The WP29 cautions ICANN 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.

Lawfulness of processing

The WP29 notes that the Final Interim Model identifies four different legal bases as being relevant in the context of the WHOIS system, namely:

- consent from the data subject (article 6(1)a GDPR);
- performance of a contract (article 6(1)b GDPR);
- legal obligation (article 6(1c)); and
- legitimate interests (article 6(1)f GDPR).[7]

While the WP29 welcomes ICANN's efforts to identify in greater detail which legal bases may be relevant in the context of the WHOIS system, it is clear that the legal bases are not always clearly linked to a specified purpose. The WP29 wishes to stress that while a particular processing operation might serve several purposes (and therefore can be justified on more than one legal basis), each individual purpose can only be justified with reference to one legal basis.[8] The WP29 therefore encourages ICANN to specify more clearly the envisaged relationship between the legitimate purposes of the processing and the relevant legal bases. For example, the Attachments to the Final Interim Model repeatedly refer to article 6(1)a of the GDPR (consent) as a basis for the processing, even in cases where the collection and/or retention of the relevant data elements shall be mandatory. As the WP29 has already indicated, consent shall only be valid to the extent that it satisfies the requirements of article 7 GDPR (including the absence of conditionality and the right to withdraw consent at any time)[9][10].

Access to non-public WHOIS data

The WP29 reiterates that any publication of WHOIS data relating to a natural person must be necessary to achieve the legitimate, specified and explicit purposes which are to be determined clearly by ICANN (e.g., ensuring registrants can be contacted in the event that there are technical issues related to a registered domain name). That publication must also be based on a legal ground as defined in article 6(1) GDPR. In this regard, the WP29 welcomes the proposal to significantly reduce the types of personal data that shall be made publically available, as well as its proposal introduce alternative methods to contact registrants or

---

[7] See Attachment 1 and 2 of the Final Interim Model.

[8] See WP29, Guidelines on Consent under Regulation 2016/679. On p. 9 of the Final Interim Model, ICANN does for example distinguish between the legal basis for the initial collection of registrant data (original purpose) and the legal basis for disclosure to third parties that request access to certain WHOIS data, such as law enforcement authorities (other purpose). The WP29 encourages ICANN to apply such distinctions in a consistent and systematic manner.

[9] See WP29, Guidelines on Consent under Regulation 2016/679.

[10] In this respect, the WP29 notes that the Registrar Accreditation Agreement currently requires registrars to obtain consent for publication of WHOIS-data. Further to its letter of 11 December 2017, the WP29 urges ICANN to reconsider this clause so as to ensure "consent" is only sought where it meets the requirements of article 7 GDPR, in particular the absence of conditionality.

administrative and technical contacts, without public disclosure of registrants' personal email addresses (referred to as "anonymized email, web form, or other technical means").

The WP29 also welcomes the fact that the Final Interim Model involves layered access and foresees an "accreditation program" for access to non-public WHOIS data.[11] That being said, important details remain absent regarding the circumstances in which access will be provided, to what extent and under which conditions and safeguards. In this regard, the WP29 takes note of ICANN's intention to undertake a detailed legal analysis of the layered data access model for the Registration Data Directory Service, and particularly how these legal bases correspond to each type of processing activity, purpose, and personal data element.[12] The layered approach should indeed take into consideration varying personal data elements in WHOIS data, limited open publication of certain data elements (provided it can be established that it is indeed necessary to achieve the purposes of the processing), and access by contracting parties and third parties to certain personal data elements, in each case tied to a defined purpose for which the data elements will be used, in order to ensure a legitimate basis for such processing as required under article 6 GDPR[13].

In this respect the WP29 encourages ICANN to develop appropriate policies and procedures applicable to incidental and systematic requests for access to WHOIS data, in particular for access by law enforcement entities.[14] It should also be clarified how access shall be limited in order to minimize risks of unauthorized access and use (e.g. by enabling access on the basis of specific queries only as opposed to bulk transfers and/or other restrictions on searches or reverse directory services, including mechanisms to restrict access to fields to what is necessary to achieve the legitimate purpose in question). Finally, the Working Party notes that, under the Final Interim Model, registries and registrars would be permitted (but not required by ICANN) to provide additional access to non-public WHOIS as long as it complies with the GDPR and other applicable laws.[15] The Working Party encourages ICANN to indeed develop binding contractual commitments in this respect between and among ICANN, registries and registrars, as suggested by the Final Interim Model[16].

Security

Article 32 GDPR provides that the controller and processor must implement appropriate technical and organisational measures to ensure an appropriate level of security. In Attachment 2 to the Proposed Interim Model it is indicated that "*[f]or example, access to the full data could be achieved by maintaining a whitelist of IP addresses in a central repository*".[17] In this respect, the WP29 expresses its concern that providing access to all non-public WHOIS data on this basis may not provide an appropriate level of security. It stresses the need to implement appropriate technical and organisational security measures that result in appropriate identification, authentication and authorization of the entities which are allowed to access WHOIS data. Moreover, ICANN should ensure that registrars and registries have appropriate logging and auditing mechanisms in place to detect possible misuse. Such

[11] Final Interim Model, p. 35
[12] Proposed Interim Model, p. 9.
[13] Proposed Interim Model, p. 9.
[14] The "accreditation" for incidental or systematic access to WHOIS data by law enforcement agencies might be arranged through for example Interpol or Europol, to help registries and registrars globally to ascertain the accreditation of such an agency, provided this can be done in accordance with the applicable legal frameworks.
[15] Final Interim Model, p. 39.
[16] Idem.
[17] Proposed Interim Model, p. 14.

logging mechanisms may also be necessary to ensure individuals can exercise their rights, in particular their right of access.

Retention period

The Final Interim Model provides that Registrars would continue to be required to retain the registration data for two years beyond the life of the domain name registration, unless a shorter time has been granted by a data retention waiver from ICANN.[18] In this respect, the WP29 notes that one of the models proposed in the context of the public review launched on 12 January 2018 foresaw a retention period of only 60 days.[19] The WP29 stresses that, in accordance with article 5(1)e GDPR, 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. In accordance with article 5(2) GDPR, ICANN must be able to demonstrate compliance with this principle of storage limitation. While Attachment 2 of the Final Interim Model mentions several lawful bases upon which retention may be justified, it does not explain why the data elements in question must in fact be retained for a period of 2 years. The WP29 therefore urges 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[20].

International transfers

ICANN should ensure that any transfers of personal data to third countries or international organisations comply with requirements contained in Chapter V of the GDPR. While the Final Interim Model makes reference to "data protection agreements", it does not clearly state how the legality of international transfers will be ensured.[21] The WP29 urges ICANN prioritise this issue in order to ensure an adequate protection of personal data transferred to third countries or international organisations.

Codes of conduct and accreditation

The Final Interim Model makes several reference to Codes of conduct and accreditation/ certification in relation to entities having access to non-public WHOIS data. The WP29 acknowledges that ICANN is still in the process of determining how its "accreditation program" will be organized and which path to take. The WP29 encourages ICANN to explore a wide range of mechanisms that could be used to identify third parties who have a legitimate ground for accessing non-public WHOIS data, under which conditions, and under which safeguards. Going forward, the WP29 urges ICANN to provide greater clarity as to whether said codes of conduct or accreditation/certification mechanism will in fact be mechanisms as envisaged by article 41-43 GDPR[22].

---

[18] Final Interim Model, p. 36.
[19] See p. 9 of https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf
[20] See also the letter of WP29 to Mr. John O. Jeffrey of 8 January 2014, p. 2 ("The 2013 RAA fails to specify a legitimate purpose which is compatible with the purpose for which the data was collected, for the retention of personal data of a period of two years after the life of a domain registration or six months from the relevant transaction respectively").
[21] Final Interim Model, p. 40-41.
[22] If that is in fact the case, ICANN should consider carefully all the requirements included in Chapter IV GDPR for Codes of Conduct and Certification to ensure that the envisaged mechanisms in the Final Interim Model are fully compatible with the GDPR.