

Samgöngu- og sveitarstjórnarráðuneytið
Sölvhólsgötu 7
101 Reykjavík

Reykjavík, 4. október 2019
Tilvísun: 2019091622/BFR

Efni: Umsögn Persónuverndar um drög að frumvarpi til laga um íslensk landshöfuðlén

Persónuvernd vísar til beiðni samgöngu- og sveitarstjórnarráðuneytisins, dags. 2. september 2019, þar sem óskað er umsagnar stofnunarinnar um drög að frumvarpi til laga um íslensk landshöfuðlén (mál nr. S-156/2019).

Í frumvarpsdrögunum er lagt til að sett verði lagaumgjörð um skráningarstofu landshöfuðlénsins .is og annarra landshöfuðléna sem síðar kunna að verða samþykkt og munu hafa beina skírskotun til Íslands.

Persónuvernd gerir eftirfarandi athugasemdir við efni frumvarpsdraganna.

1.

Í 5. gr. frumvarpsdraganna segir að vinnsla persónuupplýsinga, t.d. tengiupplýsinga og kennitalna, sem hinn skráði leggi í té, skráningarstofa, skráningaraðilar eða aðrir þeir sem starfi í umboði skráningarstofu, afli sjálfir eða berist frá þriðja aðila, sé heimil í þeim tilgangi að sinna skyldum samkvæmt frumvarpsdrögunum að uppfylltum skilyrðum laga um persónuvernd og vinnslu persónuupplýsinga. Í athugasemdum við ákvæðið segir meðal annars að það geymi heimild til vinnslu persónuupplýsinga og að gert sé ráð fyrir að vinnsla persónuupplýsinga takmarkist við upplýsingar sem flokkist sem tengiupplýsingar. Um sé að ræða upplýsingar á borð við nafn, heimilisfang, kennitölu o.s.frv.

Í a-lið 2. mgr. 8. gr. draganna er gert ráð fyrir að skráningarstofa skuli halda réttthafaskrá og aðrar upplýsingar sem nauðsynlegar eru vegna nafnaþjónustu. Hugtakið réttthafaskrá er skilgreint í 12. tölul. 4. gr. draganna sem miðlæg skrá þar sem fram koma upplýsingar um réttthafa léna, tengilið þeirra og nafnaþjóna. Í athugasemdum við ákvæðið segir að almennt sé talað um að skráningarstofur bjóði upp á þykka eða þunna réttthafaskrá (e. thick or thin WHOIS). Þykk réttthafaskrá innihaldi allar uppgæfnar upplýsingar um lén en þunn réttthafaskrá taki aðeins til tæknilegra, nauðsynlegra upplýsinga, s.s. um nafnaþjóna, skráningaraðila og réttthafa. Með réttthafaskrá í frumvarpsdrögunum sé átt við þykka réttthafaskrá.

Persónuvernd bendir á að sjálfstætt gildi 5. gr. draganna er afar takmarkað, ef nokkurt, enda er ljóst að falli vinnsla undir gildissvið laga um persónuvernd og vinnslu persónuupplýsinga, nr. 90/2018, eiga löggin við um vinnsluna, án þess að það sé sérstaklega tilgreint í þeim sérlögum sem vinnsla byggir á. Við mat á því hvort vinnsla persónuupplýsinganna teldist heimil samkvæmt lögum nr. 90/2018 má því ætla að liðið yrði til annarra ákvæða laganna, sem varða vinnslu persónuupplýsinga og við gætu átt hverju sinni. Sem dæmi um slík ákvæði má nefna 8. gr. frumvarpsdraganna, þar sem meðal annars er



fjallað um skyldu skráningarstofu til að halda réttthafaskrá. Ákvæði af þessu tagi þurfa ávallt að uppfylla kröfur laga nr. 90/2018 og reglugerðar (ESB) 2016/679 (almennu persónuverndarreglugerðarinnar), sem lögfest hefur verið hér á landi, sbr. 2. gr. laga nr. 90/2018, um skýrleika vinnsluheimilda. Í því felst meðal annars að tilgangur vinnslunnar sé skýr og að umfang hennar sé ákveðið í lögunum sjálfum, fremur en í athugasemdum við frumvarpið.

Í þessu samhengi má benda á að í athugasemdum við 5. gr. frumvarpsdraganna eru tilgreindar þær persónuupplýsingar sem ráðgert er að safnað verði samkvæmt lögunum. Þá koma einnig fram vísbendingar um upplýsingasöfnun í athugasemdum við 4. gr. frumvarpsdraganna, þar sem segir að með hugtakinu réttthafaskrá sé „átt við þykka réttthafaskrá“, sem „innihaldi allar uppgæfnar upplýsingar um lén“.

Persónuvernd bendir á að við vinnslu persónuupplýsinga skal þess meðal annars gætt að persónuupplýsingar séu nægilegar, viðeigandi og ekki umfram það sem nauðsynlegt er miðað við tilgang vinnslu, sbr. 3. tölul. 1. mgr. 8. gr. laga um persónuvernd og vinnslu persónuupplýsinga, nr. 90/2018. Ekki verður séð að tilgangur fyrirhugaðrar upplýsingaöflunar hafi verið tilgreindur með skýrum hætti í frumvarpsdrögunum. Er það mat Persónuverndar að tilgreina þyrfti á skýran hátt í lagatexta hvaða upplýsingar beri að skrá í réttthafaskrá og í hvaða tilgangi.

2.

Persónuvernd vekur athygli samgöngu- og sveitastjórnarráðuneytisins á því að svokallaður 29. gr. vinnuhópur ESB (vinnuhópur forstjóra evrópskra persónuverndarstofnana, sem starfaði á grundvelli tilskipunar 95/46/EB) og síðar Evrópska persónuverndarráðið, sem Ísland á sæti í, hafa átt í bréfaskiptum við ICANN í því skyni að tryggt verði að WHOIS-skrár og þjónusta samræmist reglugerð (ESB) 2016/679.

Persónuvernd leggur til að við frumvarpsgerðina verði tekið tillit til þeirra sjónarmiða sem fram koma í bréfi 29. gr. vinnuhópsins til ICANN, dags. 11. apríl 2018, og í bréfi Evrópska persónuverndarráðsins til ICANN, dags. 5. júlí 2018. Afrit af bréfunum eru hjálögð.

3.

Fram kemur í frumvarpsdrögunum að áhrifamat sé í vinnslu. Persónuvernd leggur til að hugað verði að gerð mats á áhrifum á persónuvernd, sem þætti í almennu áhrifamati í tengslum við frumvarpsgerðina, líkt og heimilt er samkvæmt 10. mgr. 35. gr. reglugerðar (ESB) 2016/679.

Tekið skal fram að umsögn þessi tekur aðeins til persónuupplýsinga, sbr. 2. tölul. 3. gr. laga nr. 90/2018, og vinnslu þeirra, sbr. 4. tölul. sömu greinar, en ekki annarra upplýsinga, svo sem um lögaðila.

Ekki eru að öðru leyti gerðar athugasemdir við efni draganna, að svo stöddu. Verði frekari umsagnar óskað um einstök atriði verður hún fúslega veitt. Þá áskilur Persónuvernd sér rétt til að koma á framfæri frekari athugasemdum við þinglega meðferð málsins, telji hún þörf á.



F.h. Persónuverndar,

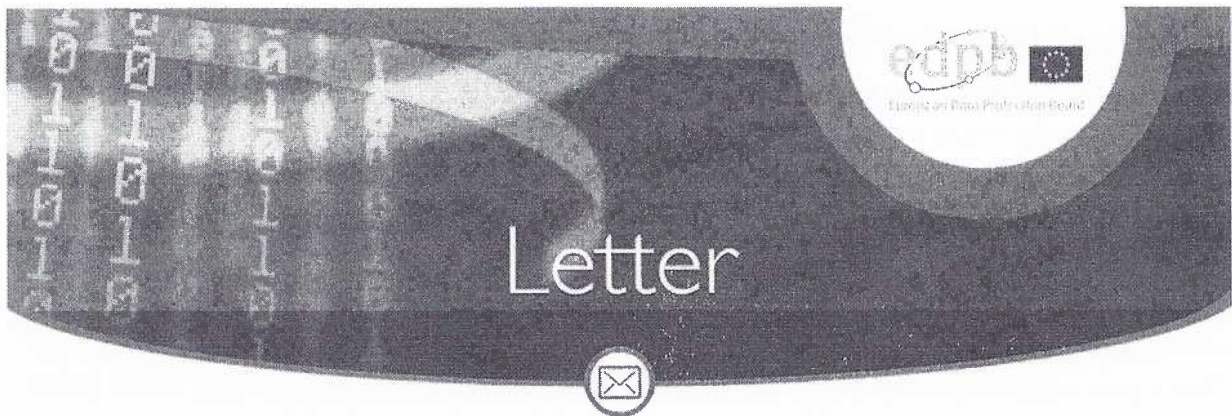

Vigdís Eva Línal


Bjarni Freyr Rúnarsson

Hjálagt:

Afrit bréfs 29. gr. vinnuhóps ESB til ICANN, dags. 11. apríl 2018.

Afrit bréfs Evrópska persónuverndarráðsins til ICANN, dags. 5. júlí 2018.



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*” 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/gdpr-compliance-interim-model-08mar18-en.pdf>.

⁹ Idem.

¹⁰ ICANN, English translation of Motion for the issuance of a preliminary injunction, *ICANN v. EPAG Domainservices, 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 EDPS.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. Steve 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



Andrea Jelinek

Chairperson

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



Brussels, 11 April 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 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 2018¹. 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

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>

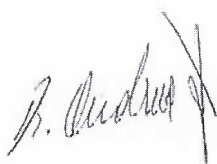
³ <https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf>

⁴ Available at <https://www.datenschutz-berlin.de/working-paper.html>

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 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

A handwritten signature in black ink, appearing to read "A. Jelinek", with a stylized flourish at the end.

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(1)c); 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 GDPR¹³.

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 Model¹⁶.

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 period²⁰.

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 to 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 GDPR²².

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.