



EN

AL-ALAC-ST-0404-01-01-EN

ORIGINAL: English

DATE: 10 April 2018

STATUS: Ratified

AT-LARGE ADVISORY COMMITTEE

ALAC Statement on Data Protection/Privacy Issues: ICANN Proposed Interim Model

Introduction

Alan Greenberg, At-Large Advisory Committee (ALAC) Chair, and Bastiaan Goslings, ALAC Vice Chair, developed an initial draft of the Statement on behalf of the ALAC.

On 31 March 2018, the first draft of the Statement was posted on its [At-Large workspace](#).

On that same date, ICANN Policy Staff in support of the At-Large Community sent a Call for Comments on the Statement to the At-Large Community via the ALAC Work mailing list.

On 02 April 2018, the ALAC Chair submitted comment. On 03 April 2018, a version incorporating additional comments received was posted on the aforementioned workspace and the ALAC Chair requested that Staff open an ALAC ratification vote.

In the interest of time, the ALAC Chair requested that the Statement be transmitted to the ICANN public comment process, copying the ICANN Staff member responsible for this topic, with a note that the Statement is pending ALAC ratification.

On 07 April 2018, Staff confirmed that the online vote results in the ALAC endorsing the Statement with 13 votes in favor, 0 vote against, and 0 abstention. Please note 86.67% (13) of the 15 ALAC Members participated in the poll. The ALAC Members who participated in the poll are (alphabetical order by first name): Alan Greenberg, Alberto Soto, Andrei Kolesnikov, Bastiaan Goslings, Holly Raiche, Javier Rua-Jovet, John Laprise, Kaili Kan, Maureen Hilyard, Ricardo Holmquist, Sebastien Bachollet, Seun Ojedeji and Tijani Ben Jemaa. 2 ALAC Members, Bartlett Morgan and Hadia Elminiawi, did not vote. You may view the result independently under: <https://www.bigpulse.com/pollresults?code=540593hgcxQ3Smixd8FxxZHYxb>.

ALAC Statement on ALAC Statement on Data Protection/Privacy Issues: ICANN Proposed Interim Model

Introduction

Following discussions over the last months, in an attempt to address the upcoming European Union's General Data Protection Regulation's impact on ICANN's contracts and particularly on the collection, retention and display of registration data in the WHOIS services, ICANN published an 'Interim Model for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation' on the 8th of March 2018 [\[1\]](#). The ALAC wishes to thank the ICANN CEO for the opportunity to reflect on the model proposed.

As stated in a blogpost from the CEO on the 21st of March:

'This next stage is critical to determine what appears in the public WHOIS, including what is collected, escrowed and transferred from registrants to registrars and registries. There are open questions about several elements in the Proposed Interim Model and it's important we determine what are the best ways to answer those in a final model.'[\[2\]](#)

On the 26th of March ICANN sent a letter [\[3\]](#) to the European Data Protection Authorities (DPA's) requesting specific guidance on the proposed Interim Compliance Model as it relates to the European Union's General Data Protection Regulation (GDPR). In the letter the DPAs are asked 'to help ICANN and the domain name registries and registrars to maintain the global WHOIS in its current form, through either clarification of the GDPR, a moratorium on enforcement or other relevant actions, until a revised WHOIS policy that balances these critical public interest perspectives may be developed and implemented.'

According to ICANN, absent this specific guidance, 'the integrity of the global WHOIS system and the organization's ability to enforce WHOIS requirements after the GDPR becomes effective will be threatened.'[\[4\]](#)

The proposed Interim Model

Many gTLD registries and registrars will doubt whether current ICANN policies and contracts requiring them to collect, create, retain, escrow, and publish a variety of data elements related to registry/registrar operations, domain name registrations, and registrants are compliant with the GDPR. Others believe that the rationales provided by ICANN, along with the intended uses are sufficient to justify collection of such elements, subject to limited publication, at least pending formal policy development. So the question is how to interpret and apply the new law to provide clear recommendations on how contracted parties operating in the EU can ensure compliance.

Layered/tiered access to WHOIS data

Notably, to comply with the GDPR the proposed Interim model requires a shift from the current requirement for gTLD registries and registrars to provide open, publicly available WHOIS services to an approach requiring a layered/tiered access model for WHOIS.

The ALAC agrees that the Interim Compliance Model's tiered access approach accommodates the interests or fundamental rights and freedoms of the data subject reflected in the domain name registration by limiting public access to the entire Thick WHOIS data.

Accreditation program to facilitate access to non-public WHOIS data

Such layered/tiered access for WHOIS means that an accreditation program of some sort for access to partial and/or full WHOIS data needs to be developed. The model suggests that this is to be done ‘in consultation with the Governmental Advisory Committee, data protection authorities and contracted parties with full transparency to the ICANN community’^[5]. Apart from the accreditation it also needs to be determined which elements of WHOIS data should only be available to which classes of accredited users.

The ALAC appreciates the suggestion that this intended endeavour be ‘fully transparent’, however it believes that the accreditation mechanism to be applied should be developed by the entire community, in a true multistakeholder fashion. Being ‘transparently’ informed afterwards is not the same as being part of the process and having the opportunity to engage and participate fully. The ALAC is also concerned with regard to the current lack of clarity when it comes to exactly what the layered/tiered model and the associated accreditation process will look like and consist of. The ALAC doubts whether the GAC should be given such a – seemingly- prominent role to establish (‘in consultation’) what the criteria for accreditation should be. Again, this should be a multistakeholder process. However, the ALAC notes that the timelines are very short, and we cannot afford to take years to do this.

A question to be addressed as part of a layered/tiered approach in the Interim Compliance Model is what data elements can continue to be published in the public layer of WHOIS. And who can then access non-public WHOIS data, and by what method? It seems to be impractical and unreasonable to require third-parties with a clear legitimate interest to obtain a court order to be granted access to non-public WHOIS data on a case-by-case basis.

Under the proposed approach, which the ALAC agrees with, user groups with a legitimate interest and who are bound to abide by adequate measures of protection, for example law enforcement agencies and intellectual property lawyers, should be able to access non-public WHOIS data based on explicit pre-defined criteria and limitations under a formal accreditation program. This approach attempts to provide a method beyond legal due process to provide continued access to full Thick WHOIS data for legitimate purposes consistent with the GDPR. Those legitimately combatting cyber abuse including spam, phishing and malware distribution must similarly be given appropriate access, but the methodology for doing so, particularly in the short term is less clear and must urgently be addressed.

As stated, the ALAC is concerned however with regard to the development of the accreditation program, the number of remaining open decision items and the very short timeline before the GDPR is applicable.

The ALAC can only stress the importance of further engagement with EU data protection authorities to define and reach agreement on an accreditation approach that satisfies the requirements of the GDPR, which approach could include the certification of codes of conduct or participation in a data protection certification. As legal analysis and response to community comments indicates.^[6]

The ALAC would like to see a reflection from the DPAs on which non-public WHOIS data should be accessible to accredited parties, whether there should be different levels of accreditation (levels of ‘layered/tiered access’, i.e. to different sets of WHOIS data) and, if so, what the associated criteria should be, and once a party is accredited how access to (a subset of) WHOIS data is provided and if that could be a form of ‘bulk’ access.

The Interim Model in the eyes of the ALAC rather casually states that ‘should the accreditation program not be ready to be implemented at the same time as the layered access model, some commentators have suggested “self-certification” as an “interim” solution, however this would raise a number of questions that would need to be addressed to comply with the GDPR’.^[7] The ALAC does not believe that self-certification is a practical solution, but also notes that an effective complete shutdown of WHOIS

while an accreditation program is being created is not a desirable outcome. The ALAC would like to know from the European DPAs what their position is on this.

Purposes of processing WHOIS data

As the Interim Model says, aside from a general requirement in the Registrar Accreditation Agreement about the use of WHOIS, there is no existing written policy articulating the purposes of WHOIS[8]. Generally, the GDPR principles relating to processing of personal data require that registrant personal data be processed lawfully and fairly, for a legitimate purpose, and that it be ‘adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.’[9]

Taking into account this purpose limitation, it is first necessary to determine the particular purposes for which the WHOIS system as a whole is intended to be used. ‘Such purposes should not be confused with the actual uses of the WHOIS system’, according to Interim Model[10]. The purposes described in the Interim Model, following community input as well as legal analysis, lead to the conclusion that all Thick WHOIS data should continue to be collected by Registrars when a domain name is registered and that this would be compliant with the GDPR.

‘It is necessary to determine if such purposes of the WHOIS system are compatible with the original purpose of collecting registrant personal data, which is performing the domain name registration under the agreement with the registrant, or whether such purposes will require a separate legal basis from the one that allowed the original collection of registrant data. While the legal basis for the processing for the original purpose is mainly “processing necessary for the performance of a contract”, the purposes of the WHOIS system relies on the legal basis of “processing necessary for the legitimate interests” of the controller(s) of the WHOIS system and third parties that request access to certain WHOIS data, such as law enforcement authorities.’[11]

The ALAC has not been able to reach consensus on whether the continued collection of the complete Thick WHOIS data set can be actually combined with being GDPR compliant. The ALAC therefore urges ICANN to learn what the European Data Protection Authorities think of this, as soon as possible, in response to the Interim Model proposed. If the continued collection of Thick WHOIS data is taken as a starting point, following the purpose description in the Interim Model, the ALAC believes this then should be considered as an interim solution, and there should be a proper analysis and complete Privacy Impact Assessment to determine which data fields are needed for specific legitimate purposes. This analysis should be part of the ongoing ‘Next-Generation gTLD Registration Directory Services to Replace WHOIS’ PDP.

Taking the continued collecting of Thick WHOIS data as a starting point though, and awaiting feedback from the European DPAs on this part of the proposed Interim Model, the ALAC agrees with the categories of data elements in the Interim Model that should (not) be made public, as described in section 7.2.8 of the Model.

The ALAC was not able to reach consensus on the proposed ‘anonymised email address or webform’ (‘Users without accreditation for full WHOIS access would maintain the ability to contact the registrant or administrative and technical contacts, either through an anonymized email, web form, or other technical and legal means’[12]). The ALAC understands the intention to not publish a registrant’s personal email-address, however views differ as to whether that intention is reasonable, implementable or effective. Some accept the requirement to anonymise addresses, but believe that the same address must be anonymised identically for all registrations within and across registrars, and the ability to recognize patterns in registration is essential to both fighting cyber abuse and to protecting against intellectual property violations. Others note that using an anonymous forwarder boils down to sending an e.g. error report ‘into a black hole’ which cannot be debugged and can effectively negate the benefit

of publishing any email address. Furthermore any response from the person in question will most likely reveal her/his real email-address (on the other hand one could argue that the sharing by the respondent of this particular contact-detail is by consent).

Continued transfers of all Thick WHOIS data from registrars to registries

ICANN org's current contracts and policies require registrars to transfer Thick registration data to the registry. This requirement for Thick data is intended to enhance accessibility and enhance stability by having the data at both the registrar and the registry. Additionally, having the full Thick WHOIS data at the registrar and registry allows for redundancy in the system to protect registrants. The GDPR expressly acknowledges processing of personal data "to the extent strictly necessary and proportionate for the purposes of ensuring network and information security" as a legitimate interest[1], which is an interest very similar to the interest in the accessibility and stability of the domain name system as the overarching reason for maintaining a Thick WHOIS system.[13]

The reasoning is seemingly sound, and the ALAC appreciates this legal analysis. However the ALAC was not able to reach consensus on whether the conclusion is indeed in compliance with what the GDPR requires. So this is another issue the ALAC hopes the European DPAs can provide clarity on as soon as possible.

Transfer of full Thick WHOIS data to escrow agents

The approach outlined in the Interim compliance proposal to continue to require registries and registrars to transfer full Thick registration data to data escrow agents for the purpose of protecting registrants in the event of registry or registrar failure or termination makes sense according to the ALAC, assuming full Thick WHOIS data continue to be transferred from registrars to registries as described above. This also fits ICANN's role to oversee the security and stability of the Internet's domain name system. In this context the ALAC thinks it is good to investigate whether a data escrow provider in Europe should be designated in order to reduce the risk faced by European registries and registrars escrowing data outside of Europe[14].

In the opinion of the ALAC there is a legitimate basis for the continued requirement for registries and registrars to transfer to data escrow agents full Thick WHOIS data. Because the purpose of processing this data is to protect registrants in the event of loss or unavailability of the registration data from the sponsoring registrar or registry, the full Thick WHOIS data set is necessary to be transferred to the data escrow provider to fulfil this purpose.

Applying the Interim Model on a global basis?

The option to apply the model on a global basis would recognize that there are data protection regulations similar to the GDPR in other jurisdictions, which in itself suggests that registries and registrars need the flexibility to apply the changes globally. It may also be difficult in practice to apply the changes to collection and processing linked to the European Economic Area (EEA) only depending upon how an individual registry or registrar has set up its systems. In general terms applying the Model globally would 'promote clarity, predictability and interoperability, which leads to supporting the public interest and the stability of the Domain Name System.[15]

The ALAC did not reach consensus on whether registrars and registries outside of the EE) should be allowed to extend the interim model to registrants outside of the EEA.

Distinction between legal and natural persons

It is not always easy to draw a clear line between personal data relating to natural or to legal persons, for example, in case of natural persons with such a close financial, personal or commercial entanglement with the legal person so that information about the legal person can be related to such natural persons. The registrations of legal persons may include personal data of natural persons, and it may also be difficult in practice to check millions of registration records and distinguish between registrations of legal and natural persons.

The ALAC did not reach consensus on whether the distinction between legal and natural persons should be mandated, and whether the model should in principle be applied to all domain name registration data contained in the WHOIS. There are those who believe that we should ensure that the maximum amount of data not covered by GDPR be available, and that the responsibility of not including personal data within legal person registration should be the responsibility of that legal person.

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

[2] <https://www.icann.org/news/blog/data-protection-privacy-issues-icann61-wrap-up-and-next-steps>

[3] E.g. <https://www.icann.org/en/system/files/correspondence/marby-to-wolfesen-26mar18-en.pdf>

[4] <https://www.icann.org/news/announcement-2018-03-28-en>

[5] Interim Model, 7.1.1, page 34

[6] Interim Model, 5.6.12, page 29

[7] Interim Model, 7.2.9.3, page 39

[8] Interim Model, 5.3.1.1, page 7

[9] Article 5(1)(c) GDPR

[10] Interim Model, 5.3.1.8, page 8

[11] Interim Model, 5.3.1.9, page 7

[12] Interim Model, 7.1.2, page 34

[13] Interim Model, 5.3.4.4, page 14

[14] Interim Model, 5.3.5.2 (community comment), page 15

[15] Interim Model, 5.4.1.2 (community comment), page 19