At-Large Workspace: IPC/BC Accreditation & Access Model for Non-Public Data v1.7

Public Comment Close	Statement Name	Status	Assignee (s)	Call for Comments Open	Call for Comments Close	Vote Open	Vote Close	Date of Submission	Staff Contact and Email	Statement Number
31 August 2018	IPC/BC Accreditation & Access Model for Non-Public Data v1.7	ADOPTED 14Y, 0N, 1A	Jonathan Zuck	31 August 2018	10 September 2018	17 September 2018	20 September 2018	10 September 2018	Steve DelBianco, Chair of ICANN's Commercial and Business Users Constituency Note: Not ICANN Staff	**AL-ALAC-ST-0818-02-01-EN**

Hide the information below, please click here >>

V1.7, 21 July 2018:

V1.6:

Note: This is not a formal ICANN Public Comment but rather an initiative spearheaded by the IPC/BC outside of ICANN, related to GDPR. At the ALAC's request, Staff have created a page on the website for IPC/BC Accreditation Model v1.4, and one on v1.5. The prior ALAC Statements related to GDPR are on the website.

To subscribe to the mailing list: https://mm.icann.org/mailman/listinfo/accred-model

See related wiki workspace on v1.5: IPC/BC Accreditation & Access Model for Non-Public Data v1.5

See related wiki workspace on v1.4: IPC/BC Accreditation & Access Model for Non-Public Data

See related website page on v1.4:
https://atlarge.icann.org/advice_statements/11537

FINAL VERSION SUBMITTED (IF RATIFIED)

The final version to be submitted, if the draft is ratified, will be placed here by upon completion of the vote.

FINAL DRAFT VERSION TO BE VOTED UPON BY THE ALAC

The final draft version to be voted upon by the ALAC will be placed here before the vote is to begin.

The At-Large Advisory Committee (ALAC) appreciates the opportunity to comment on the Draft Accreditation and Access Model (AAM). At the heart of the matter is the notion of "purpose" versus "use." The most concerning element of this version of the draft access model is that it still does not address how ICANN will handle requests from law enforcement. There are those within the ICANN community that believe we should venture back 30 years in our quest for purpose while others believe the unforeseen growth of the internet requires a broader definition of purpose in which "security and stability" includes some measure of consumer protection. End user surveys suggest that the majority of end users rely on all of the actors outlined in the proposed model to protect their interests.

Consequently, use and purpose can be difficult to distinguish in the modern era. While the ALAC agrees with the ICANN ORG presumption that the current model for data collection is the path forward in the near term, the nuance, at present, is in designing a model of accreditation and access. The ALAC understands that tiered access is the most probable solution to ensuring compliance with the General Data Protection Regulation (GDPR), but we do have serious concerns as to the structure of this proposed model. Within the current draft, the model provides an all-or-nothing approach to the data sought, where the petitioner's request and purpose may only justify access to specific non-public data. Furthermore, specific data requests may require a higher bar (for example judicial) for access. We recommend a *three-dimensional* access model of accreditation: 1) identity of the petitioner; 2) determining the petitioner's purpose; and 3) requesting information on how they will use that data. At its core, the mission of the accreditation model should be to provide a reliable and trusted domain name system (DNS) and the ALAC feels these considerations will propel the ICANN community further in that direction.

Identity of the Petitioner

As noted above, the first stage is to identify who is requesting the information. The ALAC recommends that the ICANN community should develop a system in which certain members or entities have levels of access to non-public information. The system should be very much analogous to obtaining a security clearance in the United States. Thus, depending level of access for which you qualify, determines what type of non-public data you or your organization will have access to. The ALAC is pleased that the Draft AAM envisions different categories of eligible parties, but it is still unclear as to what criteria an ICANN-approved accreditation review authority will use to determine eligibility or how much access those entities will grant them.

In equity and efficiency, until such an assessment is made, the ALAC recommends that ICANN should consider requiring the use of anonymized emails to address most of the concerns related to third-party access of such data so long as the petitioner has made a *prima facia* case that they seek the data for a legitimate purpose. We believe it serves as a way for those whom feel as though their various rights have been violated to reach out without disclosing personally identifiable information. Additionally, it allows the petitioning party to go through the accreditation process to seek the relevant data concurrently.

Although it appears the current draft of the accreditation model sets up a three-tiered system that seems to address some of these concerns, it provides little clarity as to how much access a petitioner might receive upon request. The categories are as follows: 1) regular; 2) special access; and 3) one-time access. It is unclear to the ALAC how each categories relates to the categories of legitimate reasons for access (e.g., IP investigations, Security investigations, and business investigations). Additionally, it is unclear as to how or who will ultimately make such determinations, because the AAM model does not appear to provide adequate insights into the qualifications of a member of its "Accreditation Review Panel." The ALAC requests further clarification from the drafting ICANN communities.

Defining Legitimate Purpose

The ALAC understands that the purpose of this draft model is to provide a temporary solution to comply with the E.U.'s GDPR which has been in effect on May 25, 2018. Maintaining the confidentiality and integrity of an individual's personal information, either within the E.U. or outside of it, is a priority to the ALAC. WHOIS is a multifunctional system that is invaluable for those attempting to conduct legitimate business, defend established IP rights, and protect consumers from fraud, phishing and other illegal enterprises. ICANN should promulgate a solution that balances the equities between GDPR compliant protection of personal information and the other essential functions of WHOIS. The ALAC believes that all the actors described in the proposed accreditation model play a legitimate role in a secure, sustainable and transparent DNS, enabled by a balanced AAM.

In its letter, the European Data Protection Board (EDPB), formerly WP29, provides input on ICANN's interim model and provides what it feels are measures by which ICANN can improve the model to align with the GDPR's requirements. For example, on issue of purpose specification, the EDPB notes its belief that the phrase "legitimate access..[to] accurate, reliable and uniform registration data" within the interim model's text is too broad and would, thus, violate Article 5(1)(b) of the GDPR. EDPB also recommends that ICANN better define the term "purposes" and take out the term "include" in this context to ensure that ICANN's interim model meets the comprehensive-and-exhaustive standard under Article 5. Even though we believe that EDPB's recommendation is vague, the ALAC recommends that ICANN should reiterate its considerations for legitimate purposes under in its interim model, like allowing registrars to perform basic administrative functions, security research, and specific forms of consumer protection including IP enforcement.

It appears that the recent draft AAM provides such a list consistent with the WP29's advice, but there are instances in which the draft AAM still uses the term "include" and this term should be purged in order to comply fully with the GDPR as the EDPB recommend. Additionally, by providing "examples" in various categories, it is unclear as to whether the AAM intends these proffered examples to be an exhaustive list for purposes of GDPR compliance. Therefore, the language of the AAM should make clear that either it intends these examples to be the only instances on which an ICANN-approved accreditation authority will take action or if they are actually an incomplete didactic tool.

Petitioner's Disclosure of their Intended Use of the Non-Public Data

The ALAC commends the AAM for articulating a transparency requirement, which would subject a granted petitioner to a periodic review regarding appropriateness of continued access. However, the ALAC recommends that, before an ICANN-approved accreditation review authority grants a petitioner access to the non-public WHOIS data, they must disclose in detail both how they will use the data and whether they intend to give access of such information to third-parties at the outset. Although the transparency requirement might be a reasonable solution, it might allow for certain "bad" actors to misuse this periodic review as a way to circumvent initial disclosures. Thus, comprehensive initial disclosures will ensure the responsible confidentiality and integrity of the potential data subject's rights, and will provide ICANN with better information to avoid unwanted or unintended disclosures that may run afoul to certain provisions of the GDPR. Furthermore, a "purpose tier" creates another axis to balance privacy and consumer protection, allowing for different criteria for data access depending on intended use.

We appreciate the opportunity to share our views on this matter. Thank you in advance for your time and consideration on this important issue.

DRAFT SUBMITTED FOR DISCUSSION

The first draft submitted will be placed here before the call for comments begins. The Draft should be preceded by the name of the person submitting the draft and the date/time. If, during the discussion, the draft is revised, the older version(S) should be left in place and the new version along with a header line identifying the drafter and date/time should be placed above the older version(s), separated by a Horizontal Rule (available + Insert More Content control).

The At-Large Advisory Committee (ALAC) appreciates the opportunity to comment on the Draft Accreditation and Access Model (AAM). At the heart of the matter is the notion of "purpose" versus "use." The most concerning element of this version of the draft access model is that it still does not address how ICANN will handle requests from law enforcement. There are those within the ICANN community that believe we should venture back 30 years in our quest for purpose while others believe the unforeseen growth of the internet requires a broader definition of purpose in which "security and stability" includes some measure of consumer protection. End user surveys suggest that the majority of end users rely on all of the actors outlined in the proposed model to protect their interests.

Consequently, use and purpose can be difficult to distinguish in the modern era. While the ALAC agrees with the ICANN ORG presumption that the current model for data collection is the path forward in the near term, the nuance, at present, is in designing a model of accreditation and access. The ALAC understands that tiered access is the most probable solution to ensuring compliance with the General Data Protection Regulation (GDPR), but we do have serious concerns as to the structure of this proposed model. Within the current draft, the model provides an all-or-nothing approach to the data sought, where the petitioner's request and purpose may only justify access to specific non-public data. Furthermore, specific data requests may require a higher bar (for example judicial) for access. We recommend a *three-dimensional* access model of accreditation: 1) identity of the petitioner; 2) determining the petitioner's purpose; and 3) requesting information on how they will use that data. At its core, the mission of the accreditation model should be to provide a reliable and trusted domain name system (DNS) and the ALAC feels these considerations will propel the ICANN community further in that direction.

Identity of the Petitioner

As noted above, the first stage is to identify who is requesting the information. The ALAC recommends that the ICANN community should develop a system in which certain members or entities have levels of access to non-public information. The system should be very much analogous to obtaining a security clearance in the United States. Thus, depending level of access for which you qualify, determines what type of non-public data you or your organization will have access to. The ALAC is pleased that the Draft AAM envisions different categories of eligible parties, but it is still unclear as to what criteria an ICANN-approved accreditation review authority will use to determine eligibility or how much access those entities will grant them.

In equity and efficiency, until such an assessment is made, the ALAC recommends that ICANN should consider requiring the use of anonymized emails to address most of the concerns related to third-party access of such data so long as the petitioner has made a *prima facia* case that they seek the data for a legitimate purpose. We believe it serves as a way for those whom feel as though their various rights have been violated to reach out without disclosing personally identifiable information. Additionally, it allows the petitioning party to go through the accreditation process to seek the relevant data concurrently.

Although it appears the current draft of the accreditation model sets up a three-tiered system that seems to address some of these concerns, it provides little clarity as to how much access a petitioner might receive upon request. The categories are as follows: 1) regular; 2) special access; and 3) one-time access. It is unclear to the ALAC how each categories relates to the categories of legitimate reasons for access (e.g., IP investigations, Security investigations, and business investigations). Additionally, it is unclear as to how or who will ultimately make such determinations, because the AAM model does not appear to provide adequate insights into the qualifications of a member of its "Accreditation Review Panel." The ALAC requests further clarification from the drafting ICANN communities.

Defining Legitimate Purpose

The ALAC understands that the purpose of this draft model is to provide a temporary solution to comply with the E.U.'s GDPR which has been in effect on May 25, 2018. Maintaining the confidentiality and integrity of an individual's personal information, either within the E.U. or outside of it, is a priority to the ALAC. WHOIS is a multifunctional system that is invaluable for those attempting to conduct legitimate business, defend established IP rights, and protect consumers from fraud, phishing and other illegal enterprises. ICANN should promulgate a solution that balances the equities between GDPR compliant protection of personal information and the other essential functions of WHOIS. The ALAC believes that all the actors described in the proposed accreditation model play a legitimate role in a secure, sustainable and transparent DNS, enabled by a balanced AAM.

In its letter, the European Data Protection Board (EDPB), formerly WP29, provides input on ICANN's interim model and provides what it feels are measures by which ICANN can improve the model to align with the GDPR's requirements. For example, on issue of purpose specification, the EDPB notes its belief that the phrase "legitimate access..[to] accurate, reliable and uniform registration data" within the interim model's text is too broad and would, thus, violate Article 5(1)(b) of the GDPR. EDPB also recommends that ICANN better define the term "purposes" and take out the term "include" in this context to ensure that ICANN's interim model meets the comprehensive-and-exhaustive standard under Article 5. Even though we believe that EDPB's recommendation is vague, the ALAC recommends that ICANN should reiterate its considerations for legitimate purposes under in its interim model, like allowing registrars to perform basic administrative functions, security research, and specific forms of consumer protection including IP enforcement.

It appears that the recent draft AAM provides such a list consistent with the WP29's advice, but there are instances in which the draft AAM still uses the term "include" and this term should be purged in order to comply fully with the GDPR as the EDPB recommend. Additionally, by providing "examples" in various categories, it is unclear as to whether the AAM intends these proffered examples to be an exhaustive list for purposes of GDPR compliance. Therefore, the language of the AAM should make clear that either it intends these examples to be the only instances on which an ICANN-approved accreditation authority will take action or if they are actually an incomplete didactic tool.

Petitioner's Disclosure of their Intended Use of the Non-Public Data

The ALAC commends the AAM for articulating a transparency requirement, which would subject a granted petitioner to a periodic review regarding appropriateness of continued access. However, the ALAC recommends that, before an ICANN-approved accreditation review authority grants a petitioner access to the non-public WHOIS data, they must disclose in detail both how they will use the data and whether they intend to give access of such information to third-parties at the outset. Although the transparency requirement might be a reasonable solution, it might allow for certain "bad" actors to misuse this periodic review as a way to circumvent initial disclosures. Thus, comprehensive initial disclosures will ensure the responsible confidentiality and integrity of the potential data subject's rights, and will provide ICANN with better information to avoid unwanted or unintended disclosures that may run afoul to certain provisions of the GDPR. Furthermore, a "purpose tier" creates another axis to balance privacy and consumer protection, allowing for different criteria for data access depending on intended use.

We appreciate the opportunity to share our views on this matter. Thank you in advance for your time and consideration on this important issue.