ALAC Statement for EPDP Phase 1 Final Report

As demonstrated by the ALAC's long history of participating in GNSO and ICANN working groups and other processes, we strongly support and contribute to the bottom-up multistakeholder model. The ALAC participation and contributions to the EPDP further illustrate that. Moreover, the ALAC understands that any process such as this will require all parties to accept compromises.

Our support of the generic processes notwithstanding, the ALAC has significant concerns that the EPDP has not adequately addressed the issues that are most important to fulfilling critical ALAC targets in relation to the GDPR:

- Maximizing access to RDDS information for those involved with cybersecurity and consumer protection;
- Maximizing stability and resiliency of a trustworthy DNS;
- Protecting and supporting individual Internet users; and
- Protecting Registrants

There are a number of recommendations with which the ALAC has very strong concerns, and others that we find problematic. We note that some of the descriptions that follow include implementation methodologies. This is not to say that the EPDP should work at that level of detail, but to demonstrate that viable solutions do exist.

To be specific, the results with which the ALAC has very strong concern are:

- Recommendation #16: The report recommends that contracted parties will not need to perform any level of geographic differentiation due to the difficulty of determining the location of the registrant and the risk of improperly attributing a location. Given that contracted parties have claimed that accuracy of RDDS data is not an issue, the declared location of the registrant should not be questionable. And contracted parties should be able to determine where their data is being processed! Given that this issue was declared settled and not even deferred until Phase 2, the ALAC has difficulty supporting this. The ALAC is aware that there is an open question regarding whether ICANN may be considered "established" in the EU and the EPDP has requested a legal opinion. Ultimately the European Data Protection Board (EDPB) may rule and that may force the issue, but until that happens, we should not pre-judge the outcome.
- Recommendation #5: One of the original bases for WHOIS and among its current usage is to enable contact to address technical issues. The recommendation allows registrars at their option to not collect technical contact information making it difficult for registrants to identify agents to whom they delegate technical responsibility. This impacts a range of users from novices who wish to delegate their web hosting service to address technical issues to large corporations that want 24/7 coverage to address technical matters. Among the reasons for doing so is that they cannot rely on a registrants declaration that the technical contact will allow such publication,

but that ignores that a) only an anonymized address or web form would be published, and b) anyone who signs up for a mailing list is familiar with the technology asking the person who "signed up" whether they really want to do so – the same technology could be used by a registrar in this case.

- Embedded throughout the report is the concept that we will abandon the concept of Thick WHOIS. ICANN and the volunteer community recently spent considerable time and effort on the Thick WHOIS PDP which determined that there were substantial benefits to using the Thick model. This was discarded by the EPDP without due consideration of whether these benefits could justify the incorporation of this model into the GDPR solution. It was simply deemed to be "non-conforming" with GDPR without addressing the underlying rationales and alternatives.

Issues which raise considerable but somewhat lesser concern:

- All contact with registrants or their agents will be via anonymized e-mail or through web forms unless the registrant explicitly requests direct communications. This will be true in many cases even for legal persons, because the permission to redact is allowed for them (unless reversed in Phase 2). However, the sender typically gets no indication that a message is even sent, not to mention confirmation that it reached its target. It is understood that the registrar (or registry if applicable) relaying the message (relay agent) has no way of ensuring that the message is received. But in many cases, a failure is returned to the relay agent. Contracted parties must use current best practices for such actions such as copying the message originator (not displaying the actual recipient address), including a message ID that can later be used for referencing the message (including asking for confirmation of whether a bounce was received that can be identified with the sent message). The ALAC also notes that registrar/registry privacy policies must guarantee that the content of the messages it forwards will be subject to stringent privacy rules and will not be used in any way.
- Recommendations #24/25: The Inter-Registrar Transfer Policy has been very significantly weakened by the Temporary Specification and that will now continue based on the EPDP recommendations. The report does advise the GNSO to address this with "great urgency", but realistically IF the GNSO decides to charter a PDP to look at this, it will likely be 2-3 years before a solution can be implemented. That is not an acceptable risk for registrants.
- The RDDS Organization field will be redacted or deleted until a registrant approves it being displayed. Although not optimal, that solution would be acceptable if there were a guaranteed timeline associated with it.
- Recommendation #15: Data is to be retained for a period of no more than one year (with an additional cushion of 6 months to effect the deletion). The one year was based on the Transfer Dispute Resolution Process (TDRP) which gives a registrant one year to file a claim. But as a result, it is possible that the data could be deleted effectively as the claim is being filed – no buffer was allowed for processing the claim and protecting the registrant's rights. A period marginally longer than 1 year would address this, with a requirement to address TDRPs within this period.

- Recommendation #6: Registrants will be able to specify that they wish their actual contact information published, but there is no timeline for registrars to allow this, and the data may only be published by the sponsoring registrar and not by the registry (if they have the data).

On a more global level, the EPD has spent an untold amount of time discussing possible contracted party liabilities and risks associated with improperly disclosing personal information. Very little time has been spent trying to understand the risks to the DNS, the Internet and its users of NOT disclosing information in some cases. A classic example of this mindset is recommendation #17 which says that the decision on whether to differentiate legal vs natural persons should be based solely on contracted party costs and risks, and registrant privacy issues. It recommends that no consideration be given to the impact on lawful access by third parties. This lack of balance cannot produce good policy.

The term “consumer protection” occurs five times in the Temp Spec. It is not used in the present report. ”DNS Abuse” and “cybercrime” are also mentioned in the Temp Spec. “Cybercrime” is not mentioned the report, and there is one reference to addressing “DNS abuse” in Phase 2, but there is also a statement “*that it would be difficult to argue that processing to prevent DNS abuse is "necessary for the performance of a contract to which the data subject is party".”*

This lack of concern for public interest issues makes it VERY difficult to have confidence that these and other issues will be properly dealt with in Phase 2.

In determining the ALAC position on this Phase 1 Final Report, the ALAC and the EPDP At-Large support group considered our concerns over the particular issues noted here, and the concerns over how Phase 2 will be address the deferred issues as well as the access issue. An option we seriously considered was withdrawing support for the entire report based on the concerns outlined above.

Ultimately we decided we would raise objections to a small number of critical issues but would still support the report in general. We did this to demonstrate that we do support the multistakeholder process and despite concerns, we hope that the overall EPDP will consider the needs of the entire Internet community and not just focus on the needs of contracted parties and privacy advocates. What comes out of this process must be GDPR compliant. There is no question about that. But the GDPR should not be over applied and it must also allow the DNS to continue to function and to allow addressing issues of DNS abuse, cybercrime and consumer protection in a timely and effective manner.