Comment on: Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation

Submitted by: Alan Greenberg

The ALAC has not been able to come to consensus on a response in the time provided. An extension was requested by the ALAC and others, but to date, no reply has been received.

Accordingly this submission is being made solely on my own behalf.

None of the ICANN models fully meet the GDPR requirements while maintaining the utility of WHOIS to the extent possible. Model 1 (like models CM1 and CM5) comes closest in that it only applies where the GDPR applies and otherwise maintains WHOIS as it currently exists for critical, legitimate purposes including cybersecurity, anti-abuse, anti-fraud, consumer protection and IP rights protection.

From a user perspective – the prime interest of At-Large, cybersecurity, anti-abuse and anti-fraud are of paramount importance. Any implementation satisfying GDPR is going to impact this, and particularly during the initial interim implementation, but it is essential that this impact be minimized.

Model 1, however, has critical problems:

- It is likely that it will not be considered to provide sufficiently robust protection for natural persons and even more fields may need to be redacted.
- Self-certification, except in a limited number of cases with well-known cybersecurity agents or groups that already have a certification process in place (IP attorneys and law enforcement come to mind, as per Model 2) is not likely to be practical. It will create a potentially unreasonable burden on Registrars and Registries and will no doubt be implemented very unevenly. Moreover there will surely be some contracted parties who will not implement such access, and it may be that it is for those parties that we most need it. The implemented model must accommodate a full-fledged certification process when it becomes available.

The final model must address certain criteria and principles.

1. Security and stability of the Internet is crucial. We cannot sacrifice any aspect of this without due cause.
2. Current data collection must be maintained. Although collection of data is deemed to be processing and thus we can only collect data with due cause, a good case can be made that virtually all information currently collected is of use it combatting DNS abuse and preventing fraud and malware. Even if that information may only be revealed upon presentation of a subpoena or other valid legal instrument, it must have been collected first.
3. We and ICANN contracted parties must comply with the law, therefore we will have to redact some information, but that redaction must be limited to cases where the GDPR (or similar legislation in non-European jurisdictions) actually apply. Currently that means registration for natural persons in the EEA and for contracted parties in the EEA (as per ICANN Model 1)
4. We must plan for tiered, gated access and must implement that infrastructure with due haste. Any robust interim model and any final policy will have no alternative but to relay on that. The fact that we do not currently have definitions of the tiers or methods of accrediting and gating should not delay implementing the infrastructure. To avoid any doubt, I am referring to an RDAP-based solution. Moreover, we also need to develop the front-ends to use such a system, so that once we start to have the pieces in place, we can make use of them.
5. ICANN must immediately start the process to develop a robust accreditation process for those for whom full access is restricted – those on whom we depend to keep the Internet safe for users and to otherwise implement ICANN policy (such as the UDRP which relies on WHOIS access). It is unclear who will administer such a program, who will pay for it, and the criteria for becoming accredited, but that lack of clarity is exactly why we need to start the process now! Moreover, we must do this in phased manner and not wait until it is fully implemented to start accreditation. For instance, groups such as the Anti-Phishing Working Group likely have sufficient credibility to allow us to start providing them with wide access, even via special authenticated paths prior to RDAP being implemented. That will help minimize the impact of GDPR on fighting fraud and malware.
6. ICANN and its contracted parties must, once a model is decided upon, begin a pro-active publicity campaign telling registrants what we are doing. In particular we need to make them aware that we are making the natural-legal person distinction based on the WHOIS Registrant Organization field, and that for legal persons, they need to consider their contact information to ensure that these fields do not include personal information if GDPR or similar legislation applied to them (such as having a contact e-mail address in the form of firstname.lastname@...).