My response should not be seen as what should be the final outcome of this discussion on data protection laws as they impact on the requirements under the RAA and ICANN-registry agreements that personal information of registrants, inter alia, be publicly available. These comments are made in light of the necessity for ICANN Org to have an agreed interim approach on enforcement of its contracts with registries and registrars (and their resellers) before provisions of the General Data Protection Regulations (GDPR) become enforceable on 25 May 2018. Because of the very tight timeframe, I note that the emphasis for the Interim Model will not address all of the requirements of the GDPR. It will only address the most urgent of the Compliance Model elements: the direct contradiction between the contractual requirements for the publication of potentially personal information and the legal prohibitions surrounding the publication of personal information. Other elements of GDRP (and data protection requirements in other jurisdictions) are being addressed by the Registration Data Services Working Group (RDS WG).

I support the following elements of a Model for Compliance:

- Any model must be as close as possible to compliance with the GDPR and other data protection regimes. While this is an 'interim' solution with a focus on Compliance, any final decision is some time away. If registries/registrars are to change their processes, any change should be as close as possible to what a longer term policy would require.
- Any policy adopted should apply globally. Many registries/registrars outside of the EEA will have customers such that they will be covered by GDRP requirements. As well, many countries outside of the EU have similar data protection laws and are covered by similar data protection regimes.
- I accept the 'commonalities' listed for all three 'Proposed Models, with exceptions as follows:
    - On what information is collected from registrants, the GDRP and other data protection regimes have a collection minimisation principle: only personal information that is required for the data collector to carry out its function(s) should be collected. I note that, for this interim model, the assumption is that all information currently collected under contract requirements will continue to be collected. This is most likely in breach of data protection rules. The issue of what information is required by the registries/registrars is the subject of discussion - as yet unresolved - by the RDS WG. Any final compliance regime must address the issue. In the interim, however, because of the interim nature of the models, it is more important to ensure that ONLY personal information that should be accessed under data protection principles be accessed.
    - On what personal information should be available, data protection law globally would not allow the public display of all of the personal information that is currently collected and publicly available. Model 2 (A and B) would only publish the tech and Admin contacts of the registrant and only the registrant's name with their consent. Model 3 would not publish the name at all. Both Models 2 and 3 more closely comply with the GDPR and other data protection legislation. However, Model 2 does recognise need to contact the registrar/registry in legitimate situations, and also recognises that registrants may wish to have their name associated with the domain name.
    - On access to non-public data, there must be tiered access: access to personal information must be restricted to accredited parties with a legitimate and specific reason to access the data. Given the sensitivity of contact information for many individuals and organisations, a self-certification system for access would not be acceptable. As much as possible, any access must be restricted under an ICANN monitored regime. Under data protection regimes, law enforcement agencies or those operating under judicial order are given access to personal information in relation to specific factual situations. Arguably, other governmental or regulatory agencies should be given access to personal information, again in relation to specific factual situations. There may not be sufficient time to establish a formal accreditation process and agreed access procedures. As much as possible, however, ICANN must consult with all stakeholder groups, as well as data protection agencies, to develop rules on who and in what legitimate circumstances access is given to personal information of registrants.
    - There is discussion on whether the restrictions on access to personal information should apply only to natural persons or to both natural and legal persons. The difficulty with drawing such distinction is that, in the case of very small businesses or organisations, the

contact information for the legal entity amounts to personal information. This is addressed by giving registrants (natural or legal persons) the option of opting in to having their name publicly available.

- Based on the above considerations, Model 2B best balances the requirements of general data protection law with the legitimate needs for access to personal information, with the caveat that access to any personal information must be strictly limited to minimal data collected and to those with legitimate need to access personal information for a specific and limited purpose.