The Annex: Important Issues for Further Community Action "set[s] forth implementation issues raised during the course of development of this Temporary Specification for which the ICANN Board encourages the community to continue discussing so that they may be resolved as quickly as possible after the effective date of the Temporary Specification." The EPDP Team, as part of its Phase 2 deliberations, was chartered to review issues within the Annex, including,

> "2. Addressing the feasibility of requiring unique contacts to have a uniform anonymized email address across domain name registrations at a given Registrar, while ensuring security/stability and meeting the requirements of Section 2.5.1 of Appendix A."

In reviewing this topic, the Legal Committee posed the following question to its outside counsel, Bird & Bird:

> *The group has discussed the option of replacing the email address provided by the data subject with an alternate email address that would in and of itself not identify the data subject (Example: 'sfjgsdfsafgkas@pseudo.nym'). With this approach, two options emerged in the discussion, where*
> *(a) the same unique string would be used for multiple registrations by the data subject ('pseudonymisation'), or*
> *(b) the string would be unique for each registration ('anonymization').*
>
> *Under option (a), the identity of the data subject might - but need not necessarily - become identifiable by cross-referencing the content of all domain name registrations the string is used for.*
>
> *From these options, the following question arose: Under options (a) and/or (b), would the alternate address have to be considered as personal data of the data subject under the GDPR and what would be the legal consequences and risks of this determination with regard to the proposed publication of this string in the publicly accessible part of the registration data service (RDS)?*

In its summary response, Bird & Bird noted the following:

> "[Options (a) and (b) described above] would still be treated as the publication of personal data on the web. This would seem to be a case covered by a statement made in the Article 29 Working Party's 2014 Opinion on Anonymization techniques [ec.europa.eu]: "when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data." The purpose for making this e-mail address available, even though it's masked, is presumably to allow third parties to directly contact the data subject (e.g. to serve them with court summons, demand takedowns, etc.) – so it's quite clearly linked to that

particular data subject, at least so far as ICANN/Contracted Parties are concerned. However, either option would be seen as a valuable privacy-enhancing technology (OPET) / privacy by design measure."

Following the receipt of the above advice, the EPDP Legal Committee noted the risks identified in Bird & Bird's response. While the masking of personal email addresses is a "valuable privacy-enhancing technology," the publication of masked email addresses is still considered publication of personal data. Accordingly, the Legal Committee recommends the following response to the question regarding addressing the feasibility of requiring unique contacts to have a uniform masked email address across domain name registrations at a given Registrar, while ensuring security/stability and meeting the requirements of Section 2.5.1 of Appendix A:

The EPDP Team received legal guidance noting that the publication of uniform masked email addresses results in the publication of personal data; therefore, wide publication of masked email addresses is not currently feasible under the GDPR as disclosure would, in certain instances, require meaningful human review, i.e., balancing test under GDPR Article 6(1)(f).