**Small Team #1 – Legal vs. Natural Person (Status 25 October 2018)**

h)     **Applicability of Data Processing Requirements – Draft responses**

***h3) Should Contracted Parties be allowed or required to treat legal and natural persons differently, and what mechanism is needed to ensure reliable determination of status?***

The EPDP Team agrees that Contracted Parties should be allowed to treat legal and natural persons differently, but also recommends the mechanism by which this could be done should be further explored.

The EPDP Team ***does not agree*** that Contracted Parties should be ***required*** to treat legal and natural persons differently.

***h4) Is there a legal basis for Contracted Parties to treat legal and natural persons differently?***

The EPDP Team agreed that the GDPR extends protections to natural persons data and therefore would allow for Contracted Parties to treat legal persons data differently.  It should be strongly noted, however, with due regard to the communications of the EDPB, this is not a straightforward delineation, and the EPDP team should be exceptionally cautious so as not to engage in broad and invalid assumptions that in any way enhance the risk of a personal data breach occurring. Such an increased risk is not in the interests of any party. Additionally, while the focus of this EPDP is GDPR compliance, the EPDP Team noted that not all jurisdictions distinguish between legal and natural persons therefore any policy recommendations must remain flexible enough to take this into account.

***h5) What are the risks associated with differentiation of registrant status as legal or natural persons across multiple jurisdictions? (See EDPB letter of 5 July 2018).***

One important risk is that while legal persons don’t have the same protections under GDPR, natural persons employed by a legal person (and who may be designated as the registrant, admin or technical contact) are still natural persons with full rights and protections under GDPR.

The EPDP team recognises that registration data would not necessarily be subject to data protection requirements law, should such data relate purely to a legal person. It, should be noted, however, that there are many situations where it can be difficult to separate the data of natural persons from that of legal persons. This can be the case, for example, if the legal person is a sole proprietorship, if the name of a person appears in the company’s name, if the business address is a natural person’s residence, or if an email address is assigned to a single individual ( “john.doe@company.example.com” as opposed to “info@company.example.com”). The tendency to consider much company-related data as having an impact on the data protection rights of individuals can be seen in judgments of the Court of Justice of the EU (the “CJEU”) (e.g., the Bavarian Lager case, Case C-28/08 P, concerning the names of participants in a business meeting; and the Bara case, Case C201/14, concerning the processing of tax data of an individual by a public administrative body). Thus, it could be difficult in practice for ICANN to implement a policy that clearly separates the data of legal entities from personal data.

The EPDP has discussed whether this risk may be somewhat mitigated through educational resources (see recommendations). Caution has been advised, as a stated necessity to rely on educational resources may not be considered to be compatible with the concepts of privacy by default or privacy by design i.e. where additional ‘educational resources’ are deemed necessary, the process itself is likely not established or presented in a sufficiently clear manner.

The EPDP should also avoid making recommendations where it is perceived that the issue of the data subject rights can be addressed by further contractual language to be enforced against the Contracted Parties. The EPDP should focus on vindicating the rights of the data subjects and not contriving a legal mechanism to maintain a flawed delineation, where it remains clear that certainty, both legal and technological, simply doesn’t currently exist.

It is furthermore wrong to suggest that such an approach is considered to be ‘over-compliance’. It submitted that current expert opinion (i.e. the opinion of the contracted parties who are objectively the best placed to appreciate the inbuilt limitations of the current system which they themselves maintain) is that in order to ensure minimum compliance with the GDPR, we must ensure adequate controls are in place to prevent breaches (such as accidental and inadvertent publication of personal data under the false assumption that it is data of a ‘legal person’ ). It is the opinion of the contracted parties that this can currently only be achieved by applying protections to all registrants, until such a time as there are substantial advancements in the state of the art, and even then, such an imposition would only be acceptable with a full and due regard to the cost and feasibility of implementation.

It is, in the interim, acceptable were the minimum ICANN policy to make the implementation of such a delineation optional (as is currently allowed by the temporary specification); however, such a choice should rest with individual Contracted Party, and should be based on all the factors that they themselves may discern as applicable to their business model, to voluntarily assume such risk.

Additionally, the team continues to discuss what data elements are required to be collected. If data elements are required to be collected only solely to make a distinction between natural and legal persons, that represents a higher risk as that determination isn’t necessary to effect and manage a domain name registration and does not adhere to the principle of data minimization.

**Proposed Preliminary Policy Recommendation for inclusion in the Initial Report**

The EPDP Team recommends that:

* Subject to any substantial and material conclusions as a result of research as recommended below, the current temp spec wording should be generally retained.
* Although noting a distinction exists between legal and natural persons under GDPR (and other data protection laws):
  + The EPDP Team recognizes that there are technical and financial challenges in effectively making this distinction in the context of domain name registration and in the ongoing maintenance of such domains, as well as the potential implementation of any such new functionality to pre-existing registrations.
  + Additionally, other jurisdictions may protect categories of groups in a manner similar to natural persons, and the associated requirements may warrant further consideration.
* The EPDP Team recommends that GDD staff who will design the implementation of these policy recommendations should commence research by investigating how ccTLDs and contracted parties currently distinguish between natural and legal persons to inform the EPDP Team. The EPDP however cautions that such research should not be seen as an indicator as to the actual legality of such implementations, but is merely indicative as to the technology available, and the related means and methods used by such operators in making such a delineation.

* After receiving and analyzing this research, the EPDP Team will explore in a timely manner if this distinction can, or should, be made in the context of domain name registrations in a commercially reasonable and implementable way that does not result in increased liability for contracted parties.
  + If the EPDP Team concludes that the distinction can be made in such a way, it should also consider two implementation considerations, namely, if a phased approach is helpful and which data fields (if any) need to be added to accomplish this distinction. (This could require further liaising with the IETF if data fields in RDAP need to be added or changed.)

* The EPDP Team recommends that, as a best practice, registries, registrars and ICANN each develop (educational) resources available that help registrants understand the distinction between a domain name that is registered by a natural person vs. legal person / entity. These resources and communications should also encourage legal persons to provide non-personal information for their email address and other contact information. It should be noted that additional or supplemental educational resources alone should not be seen as an adequate remedy for a process that that does not clearly or adequately support the basic protect the privacy rights of a registrant.
* The EPDP team further recommends the future technical and policy creation with due regard to the preceding recommendations.