**NCSG Draft - Small Team #2 Geographic Basis (Status – 1 November 2018)**

**Charter question h1) Should Registry Operators and Registrars (“Contracted Parties”) be permitted or required to differentiate between registrants on a geographic basis?**

The EPDP Team agrees that contracted parties should be (and are) *permitted* to differentiate between registrants on a geographic basis; however, the EPDP Team members have divergent views on whether differentiation on a geographic basis should be *required*.

The Members expressing support for requiring differentiation between registrants on a geographic basis noted the following:

1. When GDPR was adopted, the global nature of the DNS was not taken into account. It therefore may be shortsighted to just focus on GDPR.
2. Applying GDPR to all registrants would undermine the ability of sovereign states to enforce their own laws and regulations within their respective jurisdictions..
3. Businesses are generally required to take into account local laws when choosing to do business with various countries; therefore, cost is not necessarily a persuasive argument to not require differentiation.

The Members opposing requiring differentiation between registrants on a geographic basis noted the following:

1. The actual location of the registrant is not alone dispositive of whether GDPR applies especially because of the widespread industry use of additional processors (e.g., backend registry service providers and resellers for registry operators and registrars, respectively).
2. Data subjects need to be informed at the time of collection about how their personal data is being processed, i.e., what data is collected, to whom it is transferred, how long it is stored, etc. Not having a common approach for all registrants could lead to two classes of registrants, which may result in competitive advantages to certain registrars/registries (due to their establishment in jurisdictions with privacy protection), fragmentation in the marketplace and interoperability issues.
3. It is often difficult to identify a registrant’s applicable jurisdiction with sufficient certainty to apply appropriate data protection rules. A differentiated treatment based on geographic location has a high likelihood of an adverse effect on the data subject’s data privacy rights through publication.
4. There are significant liability implications for Contracted Parties if they are incorrect in applying the appropriate data protection rules. Contracted parties should be free to choose whether or not to take that risk as a business decision rather than a contractual requirement.”
5. Any consensus policy needs to be commercially reasonable and implementable, and in the current market place, differentiation based on geographic location will be difficult to scale, costly, and, accordingly, neither commercially reasonable nor implementable.

**Charter question h2) Is there a legal basis for Contracted Parties to differentiate b/w registrants on a geographic basis?**

Yes, there is a legal basis for contracted parties to differentiate between registrants on a geographic basis. However, the location of the registrant alone is not a dispositive indicator if the GDPR applies. If the controller or any processor is within the EU, the GDPR will also apply.

Some members have requested ICANN, in conjunction with interested community members, to explore the feasibility of a mechanism allowing geographic differentiation (such as the EWG rules engine). [Other members of Small Team #2 did not agree to this request – to be updated, as appropriate.]

Although the law does distinguish between EEA and non EEA data, any policy must be feasible and implementable. The EWG did note in its final report that the feasibility of a rules engine would need to be tested technically. Furthermore, the EWG noted that legally, *“there are a number of open questions, especially regarding the definition, legal acceptance, and implementation of such a system”*. Given the current system and taking into account current technology and policy expectations, the inability to differentiate such data to any level of certainty, and prohibitively high implementation costs, liability risk remains too high, rendering a forced differentiation unenforceable and unimplementable.