Small Team #2 Geographic Basis

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 does not agree that differentiation on a geographic basis should be *required*. Specifically, members of the BC, IPC and GAC [add others as appropriate] have expressed the view that contracted parties should be *required* to differentiate between registrants on a geographic basis.

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 for registry operators and backend registrar service providers and resellers). For example, if a registry operator that is not subject to GDPR is using a European registry service provider as a data processor, that registry service provider has to comply with GDPR. If a registrar that is not subject to GDPR has a reseller that is subject to GDPR, either because it is located in Europe or offers services to European data subjects, that registrar would need to comply with GDPR. If a registrar uses another registrar as a service provider to run the technical operations of its registrar business, the same complexity exists.

2. 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 for registry operators and backend registrar service providers and resellers).

3. 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

Deleted: be at least

Deleted: re is not agreement

Commented [1]: I have no idea if the GDPR drafters did or did not take DNS into account. This factual statement needs a citation. If the proponent can't provide one, it should be deleted. (It's also possible that the intended meaning is different; in that case, it should be revised to be correct.)

Deleted: role

Deleted: be able to

Commented [2]: The original statement is very definitive and factual so needs a citation to source. If one can't be provided, we need to make the statement less definitive.

Deleted: always

Deleted: not expressing support for

Deleted: and resellers

Deleted: registrars, respectively

Moved (insertion) [1]

Deleted: I

Commented [MK3]: Updated language as mentioned by Kristina during the meeting.

Moved up [1]: For example, If a registry operator that is not subject to GDPR is using a European registry service provider as a data processor, that registry service provider has to comply with GDPR. If a registrar that is not subject to GDPR has a reseller that is subject to GDPR, either because it is located in Europe or offers services to European data subjects, that registrar would need to comply with GDPR. If a registrar uses another registrar as a service provider to run the technical operations of its registrar business, the same complexity exists.¶

(due to their establishment in jurisdictions with privacy protection), fragmentation in the marketplace and interoperability issues.

4. 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.
5. 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.”
6. 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.

Deleted: .

Deleted: <#>¶

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 b/w 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.

Members of the BC [add others as appropriate] have requested ICANN, in conjunction with interested community members, 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.]

Commented [4]: RySG believes this paragraph should be deleted. If it remains, however, the RySG wants the proposed language included.

Although the law does distinguish between EEA and non EEA data, any policy must be feasible and implementable. 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.