**Geographic application – Input received to date (1 November 2018)**

**Small Team #2 Geographic Basis – updated (8 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*. Specifically, members of the BC and IPC 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. GDPR should not be over-applied, i.e., not applied to personally identifiable information not falling under EEA jurisdiction.
2. The global nature of DNS data and the application and fulfillment of the Purposes, as stated herein, necessitate the application of the laws as they exist within each relevant jurisdiction.
3. Applying GDPR to all registrants would undermine the ability of sovereign states to enforce their own laws and regulations within their respective jurisdictions.
4. Businesses, including contracted parties, presumably 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 dispositive as to whether GDPR applies due to the industry use of globally dispersed 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. GDPR requires that data subjects are 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 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.

Some members have suggested ICANN, in conjunction with interested community members, should explore the feasibility of a mechanism allowing geographic differentiation (such as postulated by the EWG rules engine that was proposed by ICANN’s [Expert Working Group on gTLD Directory Services (EWG)](https://protect-us.mimecast.com/s/q1PLCL9DwzTw5n9IBi-GG?domain=community.icann.org) in 2014, at pages 87-89 of the [EWG Final Report](https://protect-us.mimecast.com/s/0BETCM8gxACkG43hkMEyo?domain=icann.org)). Others do not support such a request as part of the EPDP Team’s work because although the law does distinguish between EU/EEA and non-EU/EEA personal data, any proposed policy recommendations must be feasible and implementable. The EWG did note in its [final report](https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf) 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.

Original Language

**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). i
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 (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.

**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.]

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.

|  |
| --- |
| **NCSG** |
| The NCSG draft is a follow-up to the one provided by the RySG, with which the NCSG is largely in agreement with, but have made a few additional proposed amendments.  A discussion over email among Small Team 2 members proposed that there is no need to identify which SOs/ACs/GNSO SGs and/or Constituencies need to be identified as being in support or opposition of any of the recommendations, when publication of the output of Small Team 2 is included in the EPDP Team’s initial report. The NCSG believes, for the purpose of the initial report, that this might serve as a distraction from the actual policy issue under question, and would prefer that the focus be on substance, rather than which group is advocating which position. We have therefore deleted all references to the groups in the attached draft.  The NCSG also agrees with the RySG that the last two paragraphs in the attached document, including the request for ICANN to explore the feasibility of a mechanism allowing geographic differentiation be removed. In the event that they are not, the NCSG has inserted additional text in the last paragraph, which we believe provides additional insight from the EWG on limitations regarding a potential, and so far theoretical, rules engine to serve the purpose of geographic differentiation. |
| **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. |

|  |
| --- |
| **IPC** |
| It is the IPC's position that it is important and feasible for contracted parties to differentiate between legal and natural persons. We believe that this distinction is supported and encouraged by the construct of the GDPR and that is valuable for all parties in the practical application of the law as it relates to WHOIS and the DNS framework and ecosystem.  The IPC submits the attached redline with further output and clarification for consideration by the team. |
| h **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. GDPR should not be over-applied. GDPR only applies to EU and EEA countries.  2. The global nature of DNS data and the application and fulfillment of the Purposes, as stated herein, necessitate the application of the laws as they exist within each relevant jurisdiction.  3. Applying GDPR to all registrants would undermine the ability of sovereign states to  enforce their own laws and regulations within their respective jurisdictions.  4. Businesses are generally required to take into account local laws when choosing to do  business with various countries; therefore, cost is not 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  (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.  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 and IPC have requested ICANN, in conjunction with  interested community members, explore the feasibility of a mechanism allowing geographic  differentiation (such as, the EWG rules engine which is presently available and applied in other law-based systems where geographic location is a factor of contractual law application. Specifically, a rules engine, similar to what was proposed by ICANN’s [Expert Working Group on gTLD Directory Services (EWG)](https://protect-us.mimecast.com/s/q1PLCL9DwzTw5n9IBi-GG?domain=community.icann.org) in 2014, at pages 87-89 of the [EWG Final Report](https://protect-us.mimecast.com/s/0BETCM8gxACkG43hkMEyo?domain=icann.org).    [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. 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. |

|  |
| --- |
| **RrSG** |
| we agree with the comments added into the working draft by Kristina and strongly support the comment on the last paragraph of the document by either being deleted or to insert Kristina’s text as noted. |

|  |
| --- |
| **RySG** |
| The RySG supports the proposed changes put forth by NCSG and opposes the proposed changes put forth by IPC. |