

<p>Small Team #2 [Fri 5 October] 13.00 – 15.00 UTC</p>	<p>Charter Questions to be addressed:</p> <p>h) Applicability of Data Processing Requirements</p> <p>h1) Should Registry Operators and Registrars (“Contracted Parties”) be permitted or required to differentiate between registrants on a geographic basis?</p> <p>h2) Is there a legal basis for Contracted Parties to differentiate between registrants on a geographic basis?</p>
<p>GDPR, Article 2, Material Scope</p>	<p>2. This Regulation does not apply to the processing of personal data:</p> <p>(a) in the course of an activity which falls outside the scope of Union law;</p> <p>(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;</p> <p>(c) by a natural person in the course of a purely personal or household activity;</p> <p>(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.</p> <p>3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.</p> <p>4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.</p>
<p>UK Information Commissioner’s</p>	<p>Who does the GDPR apply to?</p> <ul style="list-style-type: none"> • The GDPR applies to ‘controllers’ and ‘processors’.

<p>Office – Key Definitions Explanation</p>	<ul style="list-style-type: none"> • A controller determines the purposes and means of processing personal data. • A processor is responsible for processing personal data on behalf of a controller. • If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. • However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR. • The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU. • The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.
<p>Relevant Temporary Specification Sections</p>	<p>Appendix A - Requirements for Processing Personal Data in Public RDDS Where Processing is Subject to the GDPR</p> <p>2. Requirements for Processing Personal Data in Public RDDS Where Processing is Subject to the GDPR</p> <p>2.1. Registry Operator (except where Registry Operator operates a "thin" registry) and Registrar MUST apply the requirements in Sections 2 and 4 of this Appendix to Personal Data included in Registration Data where:</p> <ul style="list-style-type: none"> i. the Registrar or Registry Operator is established in the European Economic Area (EEA) as provided in Article 3(1) GDPR and Process Personal Data included in Registration Data; ii. the Registrar or Registry Operator is established outside the EEA and offers registration services to Registered Name Holders located in the EEA as contemplated by Article 3(2) GDPR that involves the Processing of Personal Data from registrants located in the EEA; or

	<p>iii. the Registrar or Registry Operator is located outside the EEA and Processes Personal Data included in Registration Data and where the Registry Operator or Registrar engages a Processor located within the EEA to Process such Personal Data.</p> <p>3. Additional Provisions Concerning Processing Personal Data in Public RDDS Where Processing is not Subject to the GDPR</p> <p>Registry Operator and Registrar MAY apply the requirements in Section 2 of this Appendix (i) where it has a commercially reasonable purpose to do so ,or (ii) where it is not technically feasible to limit application of the requirements as provided in Section 2.1 of this Appendix.</p>
<p>Appendix A Relevant input</p>	<p>Section 2.1:</p> <p>RySG: Section 2.1 can be read as requiring every Registry Operator and Registrar to apply the requirements in Sections 2 and 4 of Appendix A to all personal data for every domain name registration. We suggest replacing the phrase “the Registrar or Registry Operator” with “such Registrar or Registry Operator” in 2.1.i through 2.1.iii.</p> <p>IPC: First, while we agree that any compliance model must be applied to all contracted parties and registrants within the EEA, we disagree that it should also be applied globally, particularly in cases of a non-EU establishment and a non-EU data subject. Contracted party expediency is not an adequate justification for a substantially overbroad application of the model that goes well beyond the territorial scope of the GDPR, and is directly contrary to ICANN’s stated aim of preserving the existing WHOIS system to the greatest extent possible. It is necessary and feasible for contracted parties to draw the necessary distinction for geography. We know this because we have members who do it, at a scale.</p> <p>NCSG: The NCSG is in general agreement with the approach to publication and redaction of registrant data outlined in Appendix A, sections 2.1 – 2.5. We believe that this approach strikes the right balance between registrant privacy rights and open public access to the data needed to fulfill ICANN’s mission.</p> <p>GAC: Section 2.1: GAC Representatives to the EPDP would like to flag that consideration of this section is still ongoing, however it would not be out of order to state that some members have voiced serious concerns about this section.</p>

SSAC: Edits are needed as follows: 1) This language appears to require RDDS operators to protect/redact data that is not covered by the GDPR. For example 2.1.ii apparently requires a registrar or registry operator located outside of the EEA who does business with some registrants inside the EEA to protect ALL of its registrants no matter where they reside. For example, a registrar that is established in the Americas and does not engage a data processor in the EEA should not be allowed to use GDPR to protect/redact the data of its registrants who reside in the Americas. The policy should allow compliance with the law, but should not allow over-compliance with or over-application of the law to cover data subjects not protected by GDPR.

Section 3:

RrSG: Given the multiple data controllers and processors involved in the domain registration process, and there is no reliable way for contracted parties to determine whether processing is subject to GDPR, a conservative approach (ie applying GDPR protections to all registrant data) is the least risky.

IPC: The IPC does not support this section for the reasons listed in our answer to Question 23. This provision should be stricken. What commercially reasonable purpose would justify this? It does not seem technically infeasible to limit the application of the Section 2 requirements in cases where GDPR or other similar privacy/data protection law does not apply. Rr/Ry should be required to publish full RDDS data when such law does not apply.

Early input feedback: Appendix A.3 of the Temporary Specification allows Registry and Registrar operators to apply GDPR obligations beyond what is required. Specifically, it allows the application of the GDPR to be applied to Registrants outside of the EEA and to registrants which are legal persons. The IPC recommends that the final Consensus Policy of the EPDP limit the modification of WHOIS accuracy and transparency requirements to personal data that explicitly falls within the scope of the GDPR.

We agree that any contract modification for compliance with GDPR must be applied to all contracted parties and registrants within the EEA. However, we disagree that it should, or even could be applied globally, particularly in cases of a non-EU establishment and a non-EU data subject. This is a substantially overbroad application of the GDPR that goes well beyond the territorial scope of the GDPR and is directly contrary to ICANN's consensus policies on WHOIS and ICANN's stated aim of preserving the existing WHOIS system to the greatest extent possible.

	<p>Second, as ICANN has acknowledged, data of “legal persons,” to the extent such data does not contain “personal data,” is not within the scope of the GDPR. The GDPR, by its own terms, expressed clearly in Article 1(1) applies only to the: “protection of natural persons with regard to the processing of personal data.” We disagree with ICANN’s position not to require a distinction between data of natural versus legal persons. Instead, the model must require such a distinction; to treat registrations of natural and legal persons the same would be overly broad and unwarranted by the GDPR and not in keeping with ICANN’s mission. Accommodating efficiency and expediency concerns of Contracted Parties is not adequate justification for an overbroad application of the GDPR. Further, while some Contracted Parties have claimed it is not feasible to draw these necessarily distinctions, we know that it is feasible for contracted parties to easily differentiate between natural and legal persons, and between registrants in the EEA and registrants elsewhere. Multiple contracted parties already do so, employing a myriad of methods. Some IPC members do the same, at scale.</p> <p>BC: BC has the following concerns with this section: This allows for Registries and Registrars to apply GDPR out of scope both geographically and to the wrong parties (e.g., to legal entities not covered by GDPR or to natural persons outside of the EU -- also not covered by GDPR).</p> <p>SSAC: This language should be stricken. It was expedient when the Temp Spec was rushed into service. The language is not appropriate in the long term.</p> <p>GAC: GAC Representatives to the EPDP would like to flag that consideration of this section is still ongoing.</p>
<p>Relevant Discussion Summary Index</p>	<p>Appendix A</p>