EPDP Triage - Group Comments by Section

This chapter is a section-by-section report of the written comment of each constituency / stakeholder group / advisory committee.

A view of these same group comments are also organized by section within an Excel spreadsheets and can be found on the EPDP's wiki space. The compilation of comments by section can be found here.

Comments from the RySG

Section 1, Scope:

Language specific to the Temporary Specification will need to be removed/adjusted. RySG has concerns about the clause at the end of the second sentence (e.g., "unless ICANN determines in its reasonable discretion that this Temporary Specification SHALL NOT control"). It's important to assess the concepts of the sections and not the specific language. As noted many items from the Temporary Specification will be replaced with Consensus Policy from this ePDP so there should be effort throughout the document to make the language and concepts evergreen and flexible and steer away from specific notes to the Temporary Specification.

Section 2, Definitions:

Language about the Temporary Specification and "Interim Model" should not be needed in the working group policy recommendations. What is meant by "Registration Data" should be discussed/defined by the working group.

Section 3, Policy Effective Date:

This is Temporary Specification specific and doesn't apply to the working group policy recommendations.

Sections 4.1-4.2, Lawfulness & Purposes of Processing gTLD Registration Data:
The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the "Mission and Scope" of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Sections 4.3, Lawfulness & Purposes of Processing gTLD Registration Data:
The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the "Mission and Scope" of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Section 4.4, 4.4.1, Lawfulness & Purposes of Processing gTLD Registration Data:
The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the "Mission and Scope" of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Section 4.4.2, Lawfulness & Purposes of Processing gTLD Registration Data:
The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the "Mission and Scope" of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Section 4.4.3, for contacting registrants:
The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the "Mission and Scope" of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Section 4.4.4, for communication & invoicing:
The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the "Mission and Scope" of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Section 4.4.5, to address technical and content issues:
The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the "Mission and Scope" of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Section 4.4.6, to address changes to the domain:
The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the “Mission and Scope” of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Section 4.4.7, regarding the voluntary provision of administrative and technical contact data:
The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the “Mission and Scope” of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Section 4.4.8, to combat abuse and protect intellectual property:
The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the “Mission and Scope” of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Section 4.4.9, to provide LEA access:
The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the “Mission and Scope” of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Section 4.4.10, zone-file data:
The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the “Mission and Scope” of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Section 4.4.11, to address business or technical failure:
The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the “Mission and Scope” of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Section 4.4.12, to facilitate dispute resolution services:
The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the “Mission and Scope” of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Section 4.4.13, to facilitate contractual compliance:

The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the "Mission and Scope" of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Section 4.5.1-4.5.5, Rationale for Processing gTLD Registration Data:

The RySG notes that given the advice received from Article 29 / EDPB, the ePDP working group should reconsider the language in Section 4. Given that that the "Mission and Scope" of the ePDP charter includes Part 1: Purposes for Processing Registration Data, the RySG feels that it is important for the working group to specifically deliberate on each of the purposes set out in Section 4.4 of the Temporary Specification.

Section 5.1-5.2, Requirements Applicable to Registry Operators and Registrars:

Generally, the RySG doesn't have concerns with section 5.1 but as noted in the previous survey this doesn't imply agreement with Appendix A which is referenced in 5.1 For section 5.2 the RySG considers SLAs and Reporting requirements to be a contractual matter that should not have been included in the temporary specification and are best left out of the ePDP policy recommendations. Also to note, this section creates an obligation that is now in the past and would need to be removed or updated

Section 5.3-5.5, Requirements Applicable to Registry Operators and Registrars:

As with other comments the references here to Appendix B and C make it difficult to fully evaluate sections 5.3 and 5.4 at this point. As with other comments the references here to Appendix B and C make it difficult to fully evaluate sections 5.3 and 5.4 at this point.

Section 5.6-5.7, Requirements Applicable to Registry Operators and Registrars:

Generally ok with these sections, but note that we will review and respond to Appendix D separately (referenced in 5.6)

Section 6.1 – 6.3.2, Regarding the requirements for Registry Operators:

Section 6.1 is acceptable as is. Section 6.2 doesn't apply as written and should be removed. Section 6.3 deals with the contractual arrangements between ICANN, registries and registrars and specifically how they structure their agreements to comply with GDPR. These should not be subject to consensus policy but rather left to contracted parties to address.

Section 7.1 – 7.1.8, Notices to Registered Name Holders Regarding Data Processing:

The RySG notes that this section is specific to Registrars and defers to them on these topics but does question how these requirements apply in cases where a reseller is involved.

Section 7.1.9 – 7.1.15, Notices to Registered Name Holders Regarding Data Processing:

The RySG notes that this section is specific to Registrars and defers to them on these topics but does question how these requirements apply in cases where a reseller is involved. The RySG does note that Registrar provision of the Registry privacy policies to registrants should be considered.

Section 7.2 – 7.2.4, Additional Publication of Registration Data:

To the extent that consent to publish is a registrar only obligation, then the RySG defers to registrars. If there is an expectation that consent to publish also applies to registries (directly or insofar as it's envisioned that consent would flow from a Registrar to a Registry), then the RySG has serious concerns about how that can be achieved in a way that is GDPR compliant. It's not clear that registrants are able to provide consent passed through a registrar to a registry to publish for third parties (i.e. admin and technical contacts). We also have concerns about how the ability to withdraw consent can reasonably be implemented in this scenario.

Section 7.3-7.4, Uniform Domain Name Dispute Resolution Policy & Transfer Policy:
The RySG notes that this section is specific to Registrars and defers to them on these topics.

Section 8.1 – 8.3, Miscellaneous :
8.1- Agreed 8.2 & 8.3 are however moot as they are specific to the TS which will expire. The discussion of all of the concepts in Appendix C will require the PDP to re-examine and establish the Joint Controller, Controller, Processor relationship(s) that exists through the domain name life cycle. So, while we agree that each of the Appendix C issues should transfer to the consensus policy discussion, they should not exist currently written.

Appendix A.1 – A1.2.2, Registration Data Directory Services:
The ePDP will need to update the language here to reflect developments in RDAP. For example, section 1.1 will no longer be needed. Section 1.2 contains language specific to RDDS search capabilities (where permitted and offered); however, the RySG would like to note that the base Registry Agreement already contains suitable language in Specification 4 Section 1.10.6: "Registry Operator will: 1) implement appropriate measures to avoid abuse of this feature (e.g., permitting access only to legitimate authorized users); and 2) ensure the feature is in compliance with any applicable privacy laws or policies." The language from the Temporary Specification is unnecessary and more burdensome to implement than the existing base Registry Agreement language.

Appendix A.2 – A2.3, Registration Data Directory Services:
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. The requirements outlined in Section 2.2 may need to be adjusted based on the specific requirements of the new RDAP Profiles, which are to be put out for Public Comment shortly. Section 2.3 requires Registry Operators and Registrars to publish certain personal data based on consent received from the registrant. However, there are no established and widely used mechanisms for obtaining or tracking this consent, or passing that consent from the Registrar to the Registry Operator. This is a matter that the ePDP Team should examine in closer detail.

Appendix A.2.4 – A2.6, Redacted Fields:
Section 2.4 requires Registry Operators and Registrars to publish certain personal data based on consent received from the registrant. However, there are no established and widely used mechanisms for obtaining or tracking this consent, or passing that consent from the Registrar to the Registry Operator. This is a matter that the ePDP Team should examine in closer detail. Further, the legitimacy of collecting and processing Tech and Admin contact data is currently the subject of ongoing litigation and may change based on advice from the EDPB. The method(s) by which Registrars provide email communication to registrants outlined in Section 2.5 should be discussed further by the ePDP team.
The RySG supports the text of Section 2.6.

Appendix A.3, Additional Provisions Concerning Processing Personal Data:
No response

Appendix A.4 – A4.2, Access to Non-Public Registration Data:
Changes to the access requirements outlined in Section 4 of Appendix A should be considered during discussions of a standardized access model, which will take place later in the ePDP, following the discussion of the other elements of the Temporary Specification and completion of the Gating Questions in the ePDP Charter.

Appendix A.5, Publication of Additional Data Fields:
Changes to the access requirements outlined in Section 4 of Appendix A should be considered during The RySG has significant concerns with the Data Processing Requirements as outlined in Appendix C of the Temporary Specification. While the RySG accepts the first part of this section, "Registrar and Registry Operator MAY output additional data fields," this acceptance does not mean that the RySG agrees to all the terms of Appendix C and reserves the right to suggest edits to or removal of certain text in Appendix C. The Data Processing Requirements contained in this section may be impacted by ePDP discussion of "registration data" and purposes.

Appendix B.1, Supplemental Data Escrow Requirements:
We do not dispute the requirement for data processing agreements between contracted parties and data escrow agents, however ICANN is currently proposing data processing terms between ICANN and the data escrow agent. That conflicts with the requirement in this section that Ry or Rr incorporate those terms into their own agreements. In addition, the structure of the existing agreements vary between new and legacy TLDs. Operationalizing this requirement has proven challenging. The ePDP needs to clarify ICANN's approach to data escrow agreements and the relationships (i.e. controller / processor) between the parties. This issue highlights the greater need to clarify roles and responsibilities of parties and the structure data sharing agreements. In addition, while we do not dispute the need for data escrow agreements and related data processing provisions as required, the RySG believes that the specifics of contracts between contracted parties and escrow agents and/or ICANN, contracted parties, and vendors, should not be subject to consensus policy but instead left to contracted parties. The RySG suggests that the escrow providers and contracted parties are best placed to work out how to operate escrow services in accordance with the GDPR.

Appendix B.2, Supplemental Data Escrow Requirements:
The requirement is valid, however, in line with the response to item 11 the roles and responsibilities of the parties must be clarified as the reference here is to the "Controller" and that may be subject to change per discussion by the ePDP. In addition, any agreement with the concepts in this section do not indicate the wholesale acceptance of Appendix C. In addition, while we do not dispute the need for data escrow agreements and related data processing provisions as required, the RySG believes that specifics of contracts between contracted parties and escrow agents and/or ICANN, contracted parties, and vendors, should not be subject to consensus policy but instead left to contracted parties. The RySG suggests that the escrow providers and contracted parties are best placed to work out how to operate escrow services in accordance with the GDPR.

Appendix B.3, Supplemental Data Escrow Requirements:

We do not dispute the requirement for data processing agreements between contracted parties and data escrow agents, however ICANN is currently proposing data processing terms between ICANN and the data escrow agent. That conflicts with the requirement in this section that Ry or Rr incorporate those terms into their own agreements. In addition, the structure of the existing agreements vary between new and legacy TLDs. Operationalizing this requirement has proven challenging. The ePDP needs to clarify ICANN's approach to data escrow agreements and the relationships (i.e. controller / processor) between the parties. This issue highlights the greater need to clarify roles and responsibilities of parties and the structure data sharing agreements. In addition, while we do not dispute the need for data escrow agreements and related data processing provisions as required, the RySG believes that specifics of contracts between contracted parties and escrow agents and/or ICANN, contracted parties, and vendors, should not be subject to consensus policy but instead left to contracted parties. The RySG suggests that the escrow providers and contracted parties are best placed to work out how to operate escrow services in accordance with the GDPR.

Appendix B.4, Supplemental Data Escrow Requirements:
NOTE: While we do not dispute the need for data escrow agreements and related data processing provisions as required, the RySG does not believe it's clear that specifics of contracts between contracted parties and escrow agents and/or ICANN, contracted parties, and vendors, should be subject to consensus policy but instead left to contracted parties. The RySG suggests that it best left to escrow providers and contracted parties to work out how to operate escrow services in accordance with the GDPR.

Appendix C, Data Processing Requirements:
COMMENT: The concept of establishing the lawful basis for processing in line with Article 6 of the GDPR is important and should be discussed. It should be the task of the EPDP to re-examine this and establish the relationship of the parties throughout the Lifecycle of a domain (Processor/controller or Joint Controller). Note however that the specific contractual negotiations and requirements therein (Art 26 or Art 28) remain out of scope of the EPDP. We also caution over specific reference to the GDPR, as the ultimate policy should reflective of general data protection principles.

Appendix C.1 – C.1.6, Data Processing Requirements:
COMMENT: The GDPR is based upon specific principles that this section attempts to capture. Understanding that the consensus policy is meant to develop practices that are inherently GDPR (and other principle-based privacy law) compliant, the principles should be embedded in any processes or policies we develop as a PDP. There is no disagreement that the concepts of this section should be discussed and included in the consensus policy; however, the EPDP team should be called upon to consider and refine the Temp Spec specific language that should not transfer to ensure unintended consequences, or overly onerous requirements.

Appendix C.2, Data Processing Requirements:
The concept of establishing the lawful basis for processing in line with Article 6 of the GDPR is important and should be discussed by the EPDP team. The discussion of all of the concepts in Appendix C will require the PDP to re-examine and establish the Joint Controller, Controller, Processor relationship(s) that exists through the domain name life cycle Each of the Appendix C issues should transfer to the consensus policy discussion, but likely require redrafting. Clarity as to the concept of 'legitimate interest' is also required. It should be also noted the EPDP cannot state categorically what a 'legitimate interest is, rather we must state the reasons grounding our belief that our legal basis for processing would be considered as legitimate, were such processing to be tested by the relevant authorities. The

EPDP may consider submission of its stated / agreed upon legitimate interests as part of an Art 40 Code of conduct referral, as engaging in such a process could provide our outputs with much higher degree of certainty .

Appendix C.3 – C3.1.6, Data Processing Requirements:
COMMENT: The concepts here are all standard with regard to security requirements of the GDPR (resiliency and reliability of systems, estc) and should be discussed in the pdp. The discussion of all of the concepts in Appendix C will require the PDP to examine and establish the Joint Controller, Controller, Processor relationship(s) that exists through the domain name life cycle. So, while each of the Appendix C issues should transfer to the consensus policy discussion, they should require further discussion and refinement. How the relationship between parties is agreed will impact how these concepts are considered and included in a consensus policy. (Noting, however, that if a joint controller agreement is appropriate, the drafting of that agreement between the parties (ICANN, RYs, and Rrs) and the associated data processing terms would be outside the scope of the EPDP, per the picket fence).

Appendix C.3.2 – C3.5.2, Data Processing Requirements:
COMMENT: The concepts here are all standard with regard to security requirements of the GDPR (resiliency and reliability of systems, estc) and should be discussed in the pdp. The discussion of all of the concepts in Appendix C will require the PDP to examine and establish the Joint Controller, Controller, Processor relationship(s) that exists through the domain name life cycle. So, while each of the Appendix C issues should transfer to the consensus policy discussion, they should require further discussion and refinement. How the relationship between parties is agreed will impact how these concepts are considered and included in a consensus policy. (Noting, however, that if a joint controller agreement is appropriate, the drafting of that agreement between the parties (ICANN, RYs, and Rrs) and the associated data processing terms would be outside the scope of the ePDP, per the picket fence).

Appendix C.3.8 – C3.10, Data Processing Requirements:
COMMENT The concepts here are all standard with regard to security requirements of the GDPR (resiliency and reliability of systems, estc) and should be discussed in the pdp. The discussion of all of the concepts in Appendix C will require the PDP to examine and establish the Joint Controller, Controller, Processor relationship(s) that exists through the domain name life cycle. So, while each of the Appendix C issues should transfer to the consensus policy discussion, they should require further discussion and refinement. How the relationship between parties is agreed will impact how these concepts are considered and included in a consensus policy. (Noting, however, that if a joint controller agreement is deemed appropriate, the drafting of that agreement between the parties (ICANN, RYs, and Rrs) and the associated data processing terms would be outside the scope of the EPDP, as per the picket fence). Further, specifying the technical standards for security, unless required for interoperability among the parties, is not necessary as GDPR does not require specific or "best in class" security. The requirement is for the security measures to fit the sensitivity of the data.

Appendix D, Uniform Rapid Suspension:
Generally the RySG does not currently have any concerns with the wording of Appendix D NOTE: As Section 1.2 refers to Registrar requirements, we shall defer to the RrSG input on this matter. It should be noted that although the RySG does not have issue with the wording in the Appendix per se, s.2 does create possible incompatibilities with the existing URS procedures, and thus this should be considered during substantive review.

Appendix E, Uniform Domain Name Dispute Resolution Policy:

Rationale: Generally the RySG does not have any concerns with the Appendix E wording; however as it relates more so to Registrars efforts we shall defer to the RrSG input on this matter. NOTE: It should be noted that although the RySG does not have issue with the wording in the Appendix per se, similar to that as noted in Appendix D, s 1.2 does create a possible incompatibility with the existing UDRP procedures, and thus this should be considered during substantive review. The RySG also notes that there is a comprehensive review of URS and UDRP underway in the RPM PDP.

Appendix F, Bulk Registration Data Access to ICANN:

Understanding that the objective of this section is to tighten the language from the base RA which allows for sending more data than the minimum required, the RySG is ok with this section. Other Comments

Appendix G.1, Supplemental Procedures to the Transfer Policy:

Sections 1.1 – 1.2 are intended as temporary, stop–gap measures. In addition, the community is already engaged in efforts to replace/modify the transfer policy and therefore these sections would not likely be considered an appropriate inclusion for the Consensus Policy

Appendix G.2, Supplemental Procedures to the Transfer Policy:

As with Sections 1.1 – 1.2, Sections 2-4 are intended as temporary, stop–gap measures. In addition, as previously noted the community is already engaged in efforts to replace/modify the transfer policy and therefore these sections would not be considered an appropriate inclusion for the Consensus Policy

Part 1 – Other – Any Further Input:

These survey responses are subject to RySG internal processes and could be modified once those processes are complete. These processes have not been completed given the short period of time between receipt of the survey questions and the deadline for their submission.

Part 2 – Other – Any Further Input:

These survey responses attempt to reflect the views of the RySG but we note that it has not gone to the full group for review / approval. Responses may need to be updated.

Part 3 – Other – Any Further Input:

These survey responses attempt to reflect the views of the RySG but we note that it has not gone to the full group for review / approval. Responses may need to be updated.

Part 4 – Other – Any Further Input:

These issues are not being considered in the Triage exercise. Please note specifically the Objectives & Goals of the GNSO scope document for the EPDP note that these matters are not for initial consideration and the focus of the EPDP team should remain on the Primary queries at this juncture.

Comments from the RrSG

Section 1, Scope:
In relation to 1.3 - ‘unless ICANN determines in its reasonable discretion that this Temp. Spec SHALL NOT control’ - agreed if it is there as a backstop for unforeseen events (such as a German court ruling that some aspects are illegal). Otherwise this should be struck in its entirety.

Section 2, Definitions:
The definition about the “Interim Model” should be struck as, once the ePDP has completed its work, no “Interim Model” will remain.

Section 3, Policy Effective Date:
We note though that the Board adopted the Temporary Specification on May 17, 2018 so for the purposes of the expiration of the Temporary Specification, it would be good to know on exactly what date would it be considered expired?

Sections 4.1 - 4.2, Lawfulness & Purposes of Processing gTLD Registration Data:
ICANN does not have a legitimate interest in unfettered WHOIS access due to its bylaws. It may, in the course of the ePDP, come to be the case that ICANN has a legitimate interest, but it must first be articulated. This is supported by recent rulings by a German court.

Sections 4.3, Lawfulness & Purposes of Processing gTLD Registration Data:
The following should be struck or amended: “ICANN’s mission directly involves facilitation of third party Processing for legitimate and proportionate purposes related to law enforcement, competition, consumer protection, trust, security, stability, resiliency, malicious abuse, sovereignty, and rights protection.” It is not ICANN’s job to provide access to data. It may be the case that it is ICANN’s job to ensure that contracted parties provide access to data and that is what this Specification should lay out, not provision of data to ICANN (who has been shown in the past to be an untrustworthy steward of data—including personal data). The following should also be struck in its entirety: “the collection of Personal Data […] is specifically mandated by the Bylaws.”. While collection may be mandated by the Bylaws, the data minimization principle (Art 5(1)(c) of GDPR) requires that Personal Data shall be ‘adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’. The collection of admin, technical and billing contacts go beyond what is necessary in relation to the purposes. The starting point ought to be data minimization and so any personal data collected ought to be minimized (noting specifically that there is no reason to collect up to three contacts and that there is no viable way to obtain consent from parties not related to the registration contract). The following should be struck or amended: “other elements of the Processing Personal Data in Registration Data by Registry Operator and Registrar, as required and permitted under the Registry Operator’s Registry Agreement with ICANN and the Registrar’s Registrar Accreditation Agreement with ICANN, is needed to ensure a coordinated, stable and secure operation”. Thin whois exists for all registries other than those who have specific policies that would give them a right to communicate with the registrant eg. .pharmacy or one of the other restricted ones and this is something that something that should be in the RRA not in the Temp Spec.

Section 4.4 - 4.4.1, Lawfulness & Purposes of Processing gTLD Registration Data:

The preamble omits concepts of ‘necessity’ (Art 6 of GDPR) such as for performance of contract, compliance with legal obligation, or for performance of a task carried out in the public interest. These concepts are relevant to data processing in relation to domain name registrations (this comment references questions 8-20 in general).

Section 4.4.2, Lawfulness & Purposes of Processing gTLD Registration Data:
4.4.2 is vaguely worded and too widely drafted, and omits concepts of necessity (see comments on 8-20 above).

Section 4.4.3, for contacting registrants:
The following should be struck from the sentences “identifying and...”. (The sentence should allow contact but not necessarily identification.)

Section 4.4.4, for communication & invoicing:
4.4.4 should be struck in its entirety. Communication between registrar and its customer is nothing to do with the WHOIS and ICANN should not be adding clauses like this to registrar contracts.

Section 4.4.5, to address technical and content issues:
The following should be amended from: “technical issues and/or errors with a Registered Name or any content or resources associated with such a Registered Name” to "technical issues associated with a Registered Name". ICANN’s mandate is security and stability. Communication with the registrant on technical issues/errors is dealt with through the publication of registrar information, not registrant information on the WHOIS. Again, ICANN shouldn’t be adding these kinds of things to registrar contracts.

Section 4.4.6, to address changes to the domain:
4.4.6 should be struck in its entirety. Communications between registry, registrar and registrant are not reliant on the WHOIS. This data processing is necessary for the fulfillment of the registration contract and is done through non-WHOIS channels. The registrar must have a means of communicating with the registrant; the registry needn’t have such a means.

Section 4.4.7, regarding the voluntary provision of administrative and technical contact data:
The wording calls to mind admin and technical contacts, which are no longer useful in fulfilling the purpose of making contact with the relevant people on administrative or technical issues - that would be the registrar of record, rather than admin and tech contacts. The Registered Name Holder has a means of publishing their own information, via their website. In addition, technical and administrative contacts that are not the registrant cannot be published by the registrar without appropriate consent, which is impossible to get.

Section 4.4.8, to combat abuse and protect intellectual property:
The following should be struck: “consumer protection” and “intellectual property protection” as they're outside of ICANN’s scope / mandate and are very much down to issues around content. ICANN’s remit is for “DNS abuse” only. “Cybercrime” may be included to the extent that it is also DNS abuse. In addition, ICANN contracts for registrars and registries require them to publish specific abuse contact information.

Section 4.4.9, to provide LEA access:
We do note the jurisdiction of specific law enforcement should be addressed.

Section 4.4.10, zone-file data:

The provision of zone files has nothing to do with WHOIS and this provision should be deleted. Zone files should be technical data only, not personal data. We question the extent to which general 'Internet users' need access to zone files, and in any event, the types of internet users who have legitimate reasons for accessing zone files should be identified (eg researchers, law enforcement, rights enforcement… others?)

Section 4.4.11, to address business or technical failure:

RrSG does not understand how WHOIS would be viewed as 'safeguarding Registered Name Holders' Registration Data in the event of business or technical failure, or other unavailability of a Registrar or Registry Operator.' - clarification is needed. Data escrow should be used as a backup and not as a means for ICANN to gain access to personal data. Unavailability is a vague term and appears to be redundant to previously mentioned "business or technical failure..."

Section 4.4.12, to facilitate dispute resolution services:

No comment

Section 4.4.13, to facilitate contractual compliance:

Contractual compliance audits do not rely on public WHOIS data and can manage audits without access to personal data. WHOIS does not exist for ICANN Compliance to exploit nor has ICANN Compliance any legitimate purpose in accessing personal data. There are also possible safeguarding issues around transfer of the data to ICANN Compliance, since they have no footprint in the EU.

Section 4.5.1-4.5.5, Rationale for Processing gTLD Registration Data:

This section should probably be replaced by a simpler concept that contracted parties must process data in compliance with GDPR. Relating only to 4.5 and not to 4.5.X, which are addressed below, a note about Data Minimization and about Consent should be added to this section. Relating only to 4.5.1: The Personal Data have not been "limited" in any way, so this word is erroneous. The list above (4.4.X) do not necessarily constitute "legitimate interests" and certainly not under the GDPR in every case. RrSG is not sure which 12-month community consultation is indicated in this section but by the time the ePDP is complete, it will be an inaccurate statement, so that should be struck. Retention times have not been defined or examined for their legitimacy. Ongoing collection of certain data points has not been justified or even examined. Data retention is a contentious issue for contracted parties that are subject to EU laws. There needs to be more justification and explanation for data retention. 4.5.1 includes a lot of 3rd party processing that we cannot really know about until after the fact in many cases (if ever) so it conflicts with 4.5.4 and 4.5.5 Relating only to 4.5.3: This is a statement of fact that is false and should be struck in its entirety.

Section 5.1-5.2, Requirements Applicable to Registry Operators and Registrars:

5.1 - The RrSG is not commenting on the substance of Appendix sections on access until after other parts are resolved 5.2 - No objections

Section 5.3-5.5, Requirements Applicable to Registry Operators and Registrars:

5.3 & 5.4 - The RrSG is not commenting on the substance of Appendix sections on access until after other parts are resolved 5.5 - No comment

Section 5.6-5.7, Requirements Applicable to Registry Operators and Registrars:
5.6 - The RrSG is not commenting on the substance of Appendix sections on access until after other parts are resolved 5.7 The requirement should be rephrased in terms of necessity for the performance of the accreditation agreement. It is understood that without access to certain data there is no way of enabling ICANN to monitor or audit compliance with contractual requirements. However, ICANN need to have a very clear and narrow purpose for that access and provide safeguards for individual registrants to prevent over-reach by ICANN or other stakeholders in accessing their data.

Section 6.1 – 6.3.2, Regarding the requirements for Registry Operators:
6.1 - The RrSG is not commenting on the substance of Appendix sections on access until after other parts are resolved   6.2 - No comment / objection   6.3.1 - OK   6.3.2 - OK, so long as the community strives to have a single, standardised approach on GDPR provisions in general, and international transfers in particular, rather than introducing further complexity into registrar businesses by having diverse terms covering the same thing as a result of lack of coordination

Section 7.1 – 7.1.8, Notices to Registered Name Holders Regarding Data Processing:
We believe broadly that these types of communications are appropriate but due to different business models amongst the registrar community, we are hesitant to specifically articulate the methods of these communications. With reference to the current language, the key issues are that (a) it shouldn't differ from typical privacy policies, and (b) “Notification” should mean we can put it on our website and reference it in our Registration Agreement.

Section 7.1.9 – 7.1.15, Notices to Registered Name Holders Regarding Data Processing:
This section is too detailed, especially for existing registrants and renewals. Registrars need only to operate in compliance with GDPR. It would be a useful instead as a guidance tool for registrars who want to understand how to comply. It's also applying European Data Protection laws to every Registrar worldwide, even those who would not be caught by GDPR (having no EU operation and not processing any EU citizens' data). It should be an obligation for registrars to comply with GDPR if it applies to their business or customers.

Section 7.2 – 7.2.4, Additional Publication of Registration Data:
Collection of additional contacts is difficult at the moment due to the complexity around gaining consent. It's also not clear whether Admin and Tech contacts are included in 'Other' contacts (ie are they subject to consent and therefore optional? or are they mandatory?). If they are mandatory, why? What is the purpose for processing these data - collection, publication, access? No one seems to need them, so how can they comply with the data minimisation principle?

Section 7.3-7.4, Uniform Domain Name Dispute Resolution Policy & Transfer Policy:
7.3 - No objections 7.4 - Appendix G takes away a key use of WHOIS, ie by gaining registrars in the event of a transfer. Also, on transfers registrars blat the registration data and replace with fresh records - which is probably better overall for data quality. Can we as registrars give some input on how this is working for us? Have any problems arisen? Are we all comfortable solely relying on the security of an auth code to verify transfer requests?

Section 8.1 – 8.3, Miscellaneous :
RrSG would appreciate some clarification regarding the provision on GAC advice to enable us to evaluate the potential impact of this provision.

Appendix A.1 – A1.2.2, Registration Data Directory Services:

i Fulfilment of 1.2.1, and the compliance of such search facilities with GDPR depend on to-be-agreed mechanisms for access and is rightfully parked at the moment. Comments for later: 1.1: Has this been done by the date listed? the date should be removed. 1.2: Searching should be allowed by domain name only. Aggregation of the personal data of every registrant into one place that is searchable is a bad idea.

Appendix A.2 – A2.3, Registration Data Directory Services:

Redaction requirements for section 2.3 of Appendix make no distinction between legal and natural persons, and therefore bring corporations and organizations into play which are not protected (or have lower levels of protection) than natural persons. Registrant Organization should optionally be redacted, if it can be determined that the Organization contains Personal Information. However, given that there is currently no field in the WHOIS data set to distinguish a legal from a natural person, the application to all registrants is the only solution that offers legal cover to contracted parties, which would otherwise be drawn into making judgment calls on whether start ups, home-based businesses, personally identifying emails and other contacts are caught by GDPR. All registries should have the option of operating a thin registry at their discretion to comply with data minimization goals. Thin registries would make things WAY simpler.

Appendix A.2.4 – A2.6, Redacted Fields:

RrSG supports the redaction, but questions whether this data should continue to be collected as they are not necessary, and do not comply with data minimization principle. In relation to 2.4 - These fields ought no longer exist unless the registrant has affirmatively requested that they exist and the registrant has provided sufficient consent to the publishing, by the registrant through the registrar, registry, and ICANN respectively, of the personal data of the respective third parties. Why ‘Other’ rather than Billing? (2.4). There is no need for 'Other'. In relation to 2.5.1.3 - RrSG applauds the sentiment, but the wording could do with a review. What does ‘feasible’ mean in this context? No system is completely resilient against hacking or other breaches. I think what we want is for contracted parties to take appropriate information security measures to protect the personal data that they process from breach or other intrusions. The response to privacy/proxy reveal requests needs more precision - what if no legitimate purpose is revealed in the request for data? In what timeframe (‘reasonable’? other?) is the registrar required to provide the data? 2.6 - doesn’t make any sense and should be struck

Appendix A.3, Additional Provisions Concerning Processing Personal Data:

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.

Appendix A.4 – A4.2, Access to Non-Public Registration Data:

A court of competent jurisdiction has decided that access to personal data was appropriate in a single case, it may not be extrapolated that either, (a) access to that personal data is appropriate in all cases, (b) access by that party to other personal data is appropriate in all cases, or (c) access by similar parties to similar data is appropriate in any case. So while 4.2 is fine as written, there are significant opportunities for ICANN or other interests to stretch the meaning of it until personal data protection is a mere collection of words with no meaning whatsoever. For example there are huge issues with the concept of giving access to a “class of third party”

Appendix A.5, Publication of Additional Data Fields:
But there should be some level of consistency / rules - we don’t want raw HTML

Appendix B.1, Supplemental Data Escrow Requirements:
This section should be struck in its entirety and carried over into a review of Escrow Agents terms by ICANN. The section is confusing as it relates escrow to WHOIS, because it's nothing to do with WHOIS. It's also up to ICANN to ensure that its Escrow Agents are compliant with GDPR, because registries and registrars have little influence on the terms of Escrow which is mandated by ICANN under the terms of our accreditation.

Appendix B.2, Supplemental Data Escrow Requirements:
There are many other circumstances where international transfers need to be considered - for example technically, when a WHOIS result is accessed from anywhere in the world there is a transfer of data to a country which may or may not qualify for adequacy (although at present the personal data has temporarily been redacted). Same goes for transfer of data between registrars and registries. I'm confused about why this is limited to Escrow, and why Escrow is even in here. A GDPR audit of Escrow provision should definitely be done, but the Temp Spec is not the place for it.

Appendix B.3, Supplemental Data Escrow Requirements:
No comment

Appendix B.4, Supplemental Data Escrow Requirements:
No comment

Appendix C, Data Processing Requirements:
Not only 'access' should be mentioned here - it is correct that processing takes place at different stages and by different parties. Collection, updating, publication, access, retention. For each of these processes, there should be a clear analysis of the purpose, and how it conforms to GDPR.

Appendix C.1 – C.1.6, Data Processing Requirements:
This section should simply reference data protection principles. Currently it is too specific to GDPR, and if GDPR is amended or updated, these would become out of date. As a separate exercise (outside of the Temp Spec) it may be worthwhile for ICANN to produce non-binding guidance for contracted parties to help them understand what the principles are.

Appendix C.2, Data Processing Requirements:
Reference should not be limited to 'legitimate interest' here, as there are other issues to consider, such as necessity for fulfilment of the contract etc. Furthermore, the document should clearly state the identity of the Data Controller(s) for the WHOIS. How would it be possible for anyone to tell whether the data subject is a child, when there is no field to reflect such information in the current data set?

Appendix C.3 – C3.1.6, Data Processing Requirements:
As stated in question 5

Appendix C.3.2 – C3.5.2, Data Processing Requirements:
As stated in question 5

Appendix C.3.8 – C3.10, Data Processing Requirements:

The RrSG understands that this section is reiterating Art 32 GDPR. However, the specific examples (3.8.1-3.8.8) should not be referenced in the specification, because they are not mandatory. They are overly specific and will quickly become out of date, and may set up unrealistic expectations in the event of a regulatory intervention. ICANN is welcome to publish non-binding guidance to help registrars comply, but each registrar is different, with diverse offerings and business models. Breach notification is an area where, potentially, ICANN could helpfully play a coordinating role and offer support. This section 3.9 could lay the foundation of a richer process that is outside of the Temp Spec. 3.10 - There should be some carve out for transfers of data that are necessary for the fulfilment of the contract of registration.

Appendix D, Uniform Rapid Suspension:

No significant issues, however a processing agreement with the dispute providers is still lacking, For example the dispute providers in Asia

Appendix E - Uniform Domain Name Dispute Resolution Policy:

No comment

Appendix F - Bulk Registration Data Access to ICANN:

No comment

Appendix G.1 - Supplemental Procedures to the Transfer Policy:

The Revised Transfer Process is working, but creates new vulnerabilities for domain theft/hijack, and leaves little recourse for disputes. The Temporary Specification has exacerbated the ineffectiveness of transfer disputes; transfer dispute have never worked well, at this point the process is basically non-existant. The RrSG recommends that after the ePDP is completed, work should be done to revise & streamline the Transfer Policy, including some provisions to support transfer disputes.

Appendix G.2 - Supplemental Procedures to the Transfer Policy:

Registry operators need to make sure their limits are able to process authcode changes in bulk

Part 1 – Other – Any Further Input:

We believe the ePDP should be guided by, not the specification or contract(s) as they currently stand, but rather with the principle of data minimization and then work from there. It is not the job of the ePDP to find ways of justifying ICANN's historical use of personal data so much as it is the job of the ePDP to find a way to recreate WHOIS (if that is what is necessary) so that it is compliant with GDPR and other privacy legislation that is enacted.

Part 2 – Other – Any Further Input:

No comment

Part 3 – Other – Any Further Input:

No comment

Part 4 – Other – Any Further Input:

No comment

Comments from the NCSG

Section 1, Scope:
There are a number of provisions in both the RA and 2013 RAA, which provide guidance on situations where contractual obligations may conflict with applicable law. The NCSG does not agree that a successor to the temporary specification should allow ICANN the sole discretion on decisions where this specification controls or overrides these provisions.

Section 2, Definitions:
No comment

Section 3, Policy Effective Date:
No comment

Sections 4.1 - 4.2, Lawfulness & Purposes of Processing gTLD Registration Data:
ICANN has neither the authority nor expertise to enforce competition or consumer protection laws, and is only one of many stakeholders in the cybersecurity ecosystem. The purpose of RDDS has never been agreed, and has been a significant source of contention at ICANN since its inception. The RDDS, whether in its present form or a past iteration, should not be viewed as or considered a substitute, replacement, or proxy for the work of governments in protecting consumers. Pursuant to the coming into enforcement of the GDPR, ICANN recognizeds that the use of data gathered for the registration of a domain name, must only be for legitimate purposes, and that policies enabling its release to third parties for consumer protection, malicious abuse issues, sovereignty concerns, and rights protection must be limited, specific, and otherwise in compliance with the GDPR. Policies and mechanisms that enable consumers, rights holders, law enforcement, and other stakeholders to access the data necessary to address and resolve uses that violate law or rights must respect the principles of proportionality and data limitation. This is necessarily more complex than former practices of releasing large amounts of personal and confidential data in the WHOIS.

Sections 4.3, Lawfulness & Purposes of Processing gTLD Registration Data:
While ICANN has a responsibility as the administrator and coordinator of the DNS to facilitate the actions, qualities, and values listed above, they are goals -- and not purposes of processing (eg. trust, consumer protection). Every business and entity engaged in activities on the Internet ought to share these values. The question that needs to be unravelled here is, which types of processing, if any, are proportionate and necessary in order to ensure that these values may be upheld?. We can agree with a requirement for the customer contact point to collect data (and relevant subsequent processing such as data escrow) but the important thing here is to distinguish between collection, use (escrow, sharing for the purpose of ensuring the name resolves, etc.), and disclosure. This section needs to be reworded to be more clear. In addition, it must be pointed out that ICANN's Bylaws need to be subject to a Privacy Impact Assessment. Some language is unclear and unnecessarily broad.

Section 4.4 - 4.4.1, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Section 4.4.2, Lawfulness & Purposes of Processing gTLD Registration Data:

Actors with a legitimate interest in the data corresponding to a particular name represent a clear case for access, provided they can be securely and appropriately identified and they can demonstrate that they will commit to protecting the data under the same terms that the providing party has collected it. Some actors may be able to present a case to obtain all data in a certain element class, for a purpose such as cybersecurity where the purpose is specific (eg. monitoring for the spreading of malware). This section is worded very broadly, and the phrase "not outweighed by the fundamental rights of ….." does not sufficiently capture the requirement for greater specificity. Briefly, a tiered directory which provides access to ranges of data elements for classes of third parties is not possible under the GDPR because of the requirement for greater specificity. This needs to be added to the specification. Wording can be provided once this principle is agreed; it requires a deeper level of specificity across several sections.

Section 4.4.3, for contacting registrants:
No comment

Section 4.4.4, for communication & invoicing:
No comment

Section 4.4.5, to address technical and content issues:
Just like ICANN is not a consumer protection organization or a business regulator, ICANN is not a content regulator. Content and/or resources associated with a Registered Name are out of scope of ICANN's mission (even if this happens to be a legitimate interest). Registration data should not be used as a mechanism to enable contact with Registered Name Holders for this purpose. We therefore request suggest the removal ofing the latter half of the sentence, "or any content or resources associated with such a Registered Name."

Section 4.4.6, to address changes to the domain:
Change the text of 4.4.6 to: "Enabling a mechanism for the chosen Registrar to communicate with or notify the Registered Name Holder of commercial or technical changes in the domain in which the Registered Name has been registered;"

Section 4.4.7, regarding the voluntary provision of administrative and technical contact data:
In principle the NCSG does not object to a Registered Name Holder opting for their contact information to be disclosed to a wide audience, however this must only happen in line with Recital 43 ('Freely Given Consent') of the GDPR, which states that consent, in order to be lawful, must be freely given and a genuine choice made by the registrant.

Section 4.4.8, to combat abuse and protect intellectual property:
The NCSG believes section 4.4.8 will be better addressed during the EPDP Team's review of the annex to the temporary specification. For now we propose that section 4.4.8 be replaced with: "Enabling verified and authorized third parties (if any) to request relevant data from registrars and registries in a secure manner to address issues involving domain name registrations"

Section 4.4.9, to provide LEA access:
No comment

Section 4.4.10, zone-file data:
No comment

Section 4.4.11, to address business or technical failure:
No comment

Section 4.4.12, to facilitate dispute resolution services:
No comment

Section 4.4.13, to facilitate contractual compliance:
No comment

Section 4.5.1-4.5.5, Rationale for Processing gTLD Registration Data:
The Processing of the limited Personal Data identified in this Temporary Specification is necessary to the extent that it is consistent with and limited to ICANN's mission. This Processing specifically includes the retention of Personal Data already collected and the ongoing collection of Personal Data. The NCSG cannot accept the language in 4.5.1, which provides a blanket endorsement of all claims of "legitimate interest" contained in unspecified consultations.

Section 5.1-5.2, Requirements Applicable to Registry Operators and Registrars:
RE: 5.1. The NCSG holds the position that the Contracted Parties are data processors only to the extent (1) necessary to fulfill the objectives which are clearly and unambiguously articulated within ICANN's mission statement; and (2) to maintain their relationships with their own customers. However, many of the requirements listed in the above-mentioned contracts are data processing requirements which are performed solely at the request of ICANN org. We kindly request additional clarity from ICANN org on how, in its view, the Contracted Parties fulfill said objectives. We would also request that items which ICANN org and the contracted parties consider "picket fence items" be clearly delineated as such.

Section 5.3-5.5, Requirements Applicable to Registry Operators and Registrars:
Contractual clauses are required in other jurisdictions besides the EU.

Section 5.6-5.7, Requirements Applicable to Registry Operators and Registrars:
No comment

Section 6.1 – 6.3.2, Regarding the requirements for Registry Operators:
No comment

Section 7.1 – 7.1.8, Notices to Registered Name Holders Regarding Data Processing:
ICANN itself is a co-controller of the RDDS data, and this relationship must also be communicated to registrants. The NCSG is concerned that this language does not recognise ICANN's historic role and ongoing responsibilities as a data controller. It is not clear from this text how ICANN org intends to explain to registrants how, when, and for what purpose(s) its compliance department will have access to personal data. It is not clear what backups of this data that ICANN may retain or order be retained, nor is it clear what data processing ICANN org may contractually require its Contracted Parties to perform. Somewhere, the data subject needs to be informed about prior scraping of personal data, and the steps that might be necessary to remove their data from the repositories of data aggregators (e.g. Domain Tools). This might be the appropriate spot.

Section 7.1.9 – 7.1.15, Notices to Registered Name Holders Regarding Data Processing:
No comment

Section 7.2 – 7.2.4, Additional Publication of Registration Data:
ICANN must clarify how it will be known that a registrant has clearly, freely, and unambiguously granted his or her consent for these additional and voluntary data processing activities to be undertaken. Moreover, it must be clearly indicated to registrants that, as specified in Section 2.3 of Appendix A, publication of the additional contact information isn't mandatory. The NCSG supports the "opt-in" approach, where such information is redacted by default.

Section 7.3-7.4, Uniform Domain Name Dispute Resolution Policy & Transfer Policy:
There are more issues concerning GDPR compliance than those noted above. The Transfer Policy should undergo a Privacy Impact Assessment or Data Protection Impact Assessment.

Section 8.1 – 8.3, Miscellaneous :
The NCSG asks that the following language be inserted into section 8.1 following "Registered Name Holder": ", beyond what is required for minimum GDPR compliance". Therefore, section 8.1 should read: "This Temporary Specification will not be construed to create any obligation by either ICANN, Registry Operator, or Registrar to any non-party to this Temporary Specification, including Registered Name Holder, beyond what is required for minimum GDPR compliance." The NCSG believes section 8.2 should be modified to reflect the following: "Modifications to Temporary Specification implementation details on this Temporary Specification MAY be modified upon a two-thirds vote of the ICANN Board to make adjustments based on further inputs, including but not limited to GAC Advice, provided that the Advice does not conflict with input provided by the Article 29 Working Party/European Data Protection Board, court orders of a relevant court of competent jurisdiction concerning the GDPR, or applicable legislation and/or regulation." For clarity, we have inserted an "s" to the end of "court order", and removed the words "Board-GAC Bylaws Consultation concerning" and "in the San Juan Communique about WHOIS and GDPR" from the first sentence.

Appendix A.1 – A1.2.2, Registration Data Directory Services:
No comment

Appendix A.2 – A2.3, Registration Data Directory Services:
No comment

Appendix A.2.4 – A2.6, Redacted Fields:
No comment

Appendix A.3, Additional Provisions Concerning Processing Personal Data:
No comment

Appendix A.4 – A4.2, Access to Non-Public Registration Data:
No comment

Appendix A.5, Publication of Additional Data Fields:
No comment

Appendix B.1, Supplemental Data Escrow Requirements:
Other provisions of the GDPR apply. Would suggest a full Data Protection Impact Assessment or Privacy Impact Assessment be done of the escrow agreements.

Appendix B.2, Supplemental Data Escrow Requirements:
No comment

Appendix B.3, Supplemental Data Escrow Requirements:
No comment

Appendix B.4, Supplemental Data Escrow Requirements:
No comment

Appendix C, Data Processing Requirements:
The NCSG has no strong opinion on this language; however we do have some concerns regarding the contents of Appendix C.

Appendix C.1 – C.1.6, Data Processing Requirements:
While including language from the GDPR on data processing requirements is useful insofar as it defines the standards that must be met, this Specification lacks detail about precisely how ICANN, the contracted parties, and other participants in the ecosystem are intended to uphold these principles. Moreover, while all parties are collectively expected to adhere to these principles at all times, there are no clear avenues prescribed for how ICANN will be informed if and when registries, registrars, their agents, or any other parties or interests (including those in section 4 referenced in this appendix, to which NCSG objected to in a previous survey) receive complaints about improper data handling practices. The process for receiving and handling such requests should be clearly defined, along with processes for escalation and opportunities for recourse / remedy for individuals who have had their rights violated.

Appendix C.2, Data Processing Requirements:
It is not clear that this section adds any value. Detail is required. Identities of the holders of domains which inherently have political, religious, or racial implications also qualify for protection as sensitive data (e.g. womensreproductiverights.com, minersagainsttrump.com) so using the example of a child here only raises questions about how to apply this overall principle.

Appendix C.3 – C3.1.6, Data Processing Requirements:
No comment

Appendix C.3.2 – C3.5.2, Data Processing Requirements:
The NCSG believes that more detail is required in this section in terms of how privacy-by-design ought to be implemented.

Appendix C.3.8 – C3.10, Data Processing Requirements:
The NCSG finds section 3.9 to be too vague to be useful. More details about the respective roles of ICANN, the registrar, the reseller, and/or other data processors need to be provided. The GDPR has a 72-hour notification requirement in the event of a data breach. Regarding section 3.10, the NCSG is unclear as to which international organizations are in question.

Appendix D, Uniform Rapid Suspension:
Access to Registered Name Holder contact data in a URS proceeding involves access to this data by: Trademark owners in the event that one URS complaint is filed on behalf of one or multiple related

companies against one Registered Name Holder, or one complaint is filed against multiple Registered Name Holders that are somehow shown to be related URS Provider in order to contact the Registered Name Holder(s) using postal address, email and fax   The NCSG does not believe that a rewrite of the URS process should take place on this EPDP Team, as it is currently being done elsewhere (GNSO Review of all RPMs for all gTLDs PDP). Moreover, it is not clear what information constitutes “contact details” in Section 2, or the specific purposes for processing such data. The NCSG believes that all questions of data access, even by Trademark owners and/or URS Providers, should be deferred until the EPDP Team deliberates on an access model/framework for Registered Name Holder data. Additionally, the EPDP Team should remain informed of progress on the review of the URS, in order to align its own future access deliberations to the outcome of the URS review.

Appendix E - Uniform Domain Name Dispute Resolution Policy:
Same as response to the question on Appendix D. The question of access to Registered Name Holder data by Trademark owners and UDRP providers should be deferred.

Appendix F - Bulk Registration Data Access to ICANN:
No comment

Appendix G.1 - Supplemental Procedures to the Transfer Policy:
NCSG defers on answering this question for the time being and might develop opinions about this section that will be relayed to the group.

Appendix G.2 - Supplemental Procedures to the Transfer Policy:
NCSG might have comments on this section in the future which might lead to changing its answer.

Part 1 – Other – Any Further Input:
No comment

Part 2 – Other – Any Further Input:
No comment

Part 3 – Other – Any Further Input:
No comment

Part 4 – Other – Any Further Input:
No comment

Comments from the ISPCP

Section 1, Scope:
There are areas in the mentioned agreements that have not been touched upon on the Temporary Specification, such as Zone File Access. There are issues with these, too, from a data protection perspective. ICANN should not sanction non-compliance with such provisions.

Section 2, Definitions:

No comment

Section 3, Policy Effective Date:
Since the Temporary Specification is not compliant with GDPR in my view, it should better not be enforced.

Sections 4.1 - 4.2, Lawfulness & Purposes of Processing gTLD Registration Data:
This section needs to be rewritten after the group has established purposes for data processing and determining in whose interest the processing occurs. This issue that ICANN has conflated its own and third party interests has been pointed out by the EDPB.

Sections 4.3, Lawfulness & Purposes of Processing gTLD Registration Data:
See above

Section 4.4 - 4.4.1, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Section 4.4.2, Lawfulness & Purposes of Processing gTLD Registration Data:
There is an issue with this as processing may take place based on different legal grounds, not only legitimate interest, see Art. 6 I b and c GDPR. Where data is processed based on legitimate interests, the question is whether that can / should be mandated by ICANN as Art. 6 I f GDPR gives the controller or processor the right to process data, but not an obligation. Also, it does not grant third party requestors any right to accessing data. This section is better redrafted when the substantive discussion has been held.

Section 4.4.3, for contacting registrants:
See above

Section 4.4.4, for communication & invoicing:
Payment and Invoicing is a matter for the registrar to handle. In most, if not all cases, invoices will be issued to the account holder and not to the registrant. Hence, this is not a matter for ICANN and the document should be silent on this.

Section 4.4.5, to address technical and content issues:
ICANN must not regulate content and therefore not establish communications channels suggesting ICANN does have a role in that area.

Section 4.4.6, to address changes to the domain:
From a legal point of view, there cannot be a one size fits all approach to this. Registries may not have such interest and leave the communication to the registrar.

Section 4.4.7, regarding the voluntary provision of administrative and technical contact data:
It is questionable whether it should be a purpose of data processing to be able to publish this data, particularly since the Temporary Specification does not require the publication of this data. Also, not all contracted parties may see the need of collecting such data in the first place. Additionally, the purposes for collecting such data, if at all, must be determined before discussing the question of publication.

Section 4.4.8, to combat abuse and protect intellectual property:

Absent details on what this framework looks like, it is not possible to endorse this purpose.It is questionable whether registration data is required to be passed on to third parties to achieve all purposes that might be included in the framework.

Section 4.4.9, to provide LEA access:
LEA needs and legal grounds for providing access need to be discussed first. Where there is a legal requirement to pass on data to LEAs, that would not even need to be included in the list of purposes. It is important to discuss whether it is legally possible / desirable to make available data to LEAs that do not have a right to request data.

Section 4.4.10, zone-file data:
This requires further discussion. The way zone file data is made available today is problematic, to say the least.

Section 4.4.11, to address business or technical failure:
No comment

Section 4.4.12, to facilitate dispute resolution services:
No comment

Section 4.4.13, to facilitate contractual compliance:
This is too broad brush. The document should be precise on why the data is needed for the various groups. There also seems to be overlap with other purposes, so some aspects might be redundant.

Section 4.5.1-4.5.5, Rationale for Processing gTLD Registration Data:
The text jumps to the conclusion that processing is proportionate without specifying the processing activities and without doing the weighing of interests.

Section 5.1-5.2, Requirements Applicable to Registry Operators and Registrars:
This needs to be updated to reflect workable timelines.

Section 5.3-5.5, Requirements Applicable to Registry Operators and Registrars:
The issue with these clauses is that the Appendixes need to be revised. Also, in 5.3. ICANN is missing as a party. There is the need for data processing agreements between ICANN and escrow agents and ICANN and the EBERO. Absent such agreements, the system cannot be compliant.

Section 5.6-5.7, Requirements Applicable to Registry Operators and Registrars:
On 5.7. ICANN needs to be more specific and explain why it needs access to registration data for compliance purposes generally. In our view, this needs to be more nuanced.

Section 6.1 – 6.3.2, Regarding the requirements for Registry Operators:
On 6.1. and 6.2. the case needs to be made why such data needs to be reported, not least to be able to inform users of such processing activity. The question is whether this is compliant with the principle of data minimization. For RRAs, DPAs need to be put in place for such processing activities that go beyond the standard operations / standard practice (e.g. where additional data is required for validation purposes). However, for the standard practice of registering domain names, Rys, Rrs and ICANN are likely joint controllers. Hence, a Joint Controller Agreement needs to be drafted and entered into

between the three parties. The JCA needs to have two versions, one „light“ version for publication and one thorough document with all details

Section 7.1 – 7.1.8, Notices to Registered Name Holders Regarding Data Processing:
This clause parrots some of the requirements established in the GDPR. There is a risk with that since the reader will assume that just working off this list will make them compliant. However, that is not the case and additionally, the statement that the registrar is a controller is inaccurate because of the joint controller situation. It would be preferable to at best name the provisions of the GDPR and leave the implementation to the contracted parties. In the alternative, a usable set of language can be produced, but that would need to be accurate and comprehensive.

Section 7.1.9 – 7.1.15, Notices to Registered Name Holders Regarding Data Processing:
See answer to previous question

Section 7.2 – 7.2.4, Additional Publication of Registration Data:
There should only be a requirement to offer a consent-based solution when consent can actually be processed in a compliant fashion through all parties involved. This is not the case at the moment.

Section 7.3-7.4, Uniform Domain Name Dispute Resolution Policy & Transfer Policy:
This answer relates to this text only, not to the appendix

Section 8.1 – 8.3, Miscellaneous :
This does not reflect the Joint Controller Situation and it should encompass the entire flows of registration data.

Appendix A.1 – A1.2.2, Registration Data Directory Services:
The time frame is likely too ambitious. Also, search capabilities are legally problematic depending on how they are designed. The design should come first and then the implementation timeframe should be determined.

Appendix A.2 – A2.3, Registration Data Directory Services:
The „Organization“ field must also be redacted as a standard since the same issues apply as for registrants. Organization data can be PII and the publication should require consent.

Appendix A.2.4 – A2.6, Redacted Fields:
This assumes that this data is required, which may only be the case in certain cases and not for all TLDs. That discussion needs to be held.

Appendix A.3, Additional Provisions Concerning Processing Personal Data:
No comment

Appendix A.4 – A4.2, Access to Non-Public Registration Data:
This section needs to be rewritten. Not all disclosure of data will take place on the basis of Art. 6 I f GDPR. Also, there is an issue with making disclosure of data mandatory with such a broad brush statement. This section is best amended when the access discussion has been held.

Appendix A.5, Publication of Additional Data Fields:

Consent must be evidenced at all levels, so a consent-based publication of data requires the existence of the technical means to process consent in a compliant fashion.

Appendix B.1, Supplemental Data Escrow Requirements:
ICANN is the controller for data escrow and the Escrow Agents are processors on behalf of ICANN. Hence, this text must be rewritten to reflect that scenario.

Appendix B.2, Supplemental Data Escrow Requirements:
Yes, with the qualification that it should be made clearer that Standard Contractual Clauses are one amongst various options to be compliant.

Appendix B.3, Supplemental Data Escrow Requirements:
Given that ICANN is the controller and the Escrow Agent is the processor, it is for ICANN to enter into such agreement governing the data processing relating to escrow.

Appendix B.4, Supplemental Data Escrow Requirements:
see answer to last question.

Appendix C, Data Processing Requirements:
The paragraph is more or less just a reflection of Art. 5 GDPR, but not an accurate one. There is no added value in quoting from the law rather than just stating what articles need to be complied with.

Appendix C.1 – C.1.6, Data Processing Requirements:
This clause is more or less a reflection of Art. 6 I f GDPR, but that suggests that this is the only legal basis that can be applied for processing. Therefore, it is not comprehensive and therefore potentially misleading.

Appendix C.2, Data Processing Requirements:
As above, basic principles of GDPR (Art. 32) are cited or paraphrased. That is of limited value.

Appendix C.3 – C3.1.6, Data Processing Requirements:
See above. Additionally, informing data subjects adequately requires information about other processing activities and not only those between registries and registrars, namely Escrow, ICANN and EBERO. Information on that needs to be provided by ICANN to be included in the information duties.

Appendix C.3.2 – C3.5.2, Data Processing Requirements:
See above.

Appendix C.3.8 – C3.10, Data Processing Requirements:
See above.

Appendix D, Uniform Rapid Suspension:
No comment

Appendix E - Uniform Domain Name Dispute Resolution Policy:
No comment

Appendix F - Bulk Registration Data Access to ICANN:

The reasons for this reporting should be explained first as domain names may also be PII and thus, this processing activity needs to be analyzed for purpose and legal ground.

Appendix G.1 - Supplemental Procedures to the Transfer Policy:

No comment

Appendix G.2 - Supplemental Procedures to the Transfer Policy:

No comment

Part 1 – Other – Any Further Input:

This survey answers are under the caveat of further related input given by the ISCP constituency

Part 2 – Other – Any Further Input:

Answers are given with the caveat that further constituency input may be provided

Part 3 – Other – Any Further Input:

The relationship between RDAP and the Transfer Policy needs to be reflected in the updated document.

Part 4 – Other – Any Further Input:

These comments are subject to any further comments the ISPCP might have.

Comments from the BC

Section 1, Scope:

BC agrees with this section and suggests the following topics for future discussion: The final policy should define and bound "reasonable discretion" to set reasonable expectations for all parties regarding ICANN's responsibilities for enforcing the final policy.

Section 2, Definitions:

No comment

Section 3, Policy Effective Date:

No comment

Sections 4.1 - 4.2, Lawfulness & Purposes of Processing gTLD Registration Data:

BC agrees with this section and suggests the following topics for future discussion: The final policy document should also explicitly note that In May 2016, the ICANN Board adopted new Bylaws, setting forth obligations to replace those specified by the original Affirmation of Commitments that expired in October 2016, these new Bylaws requiring that ICANN "use commercially reasonable efforts to enforce its policies relating to registration directory services and work with Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to generic top-level domain registration data, as well as consider safeguards for protecting such data."

Sections 4.3, Lawfulness & Purposes of Processing gTLD Registration Data:

No comment

Section 4.4 - 4.4.1, Lawfulness & Purposes of Processing gTLD Registration Data:
BC agrees with this section and suggests the following topics for future discussion: The final policy should reflect that GDPR is a law specific to EEA and that there may exist opposing law outside of the jurisdiction of GDPR; processing must comply with GDPR where applicable but not necessarily elsewhere. This is significant insofar as unnecessary compliance may place undue burden on CPs in other regions where law is different.

Section 4.4.2, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Section 4.4.3, for contacting registrants:
No comment

Section 4.4.4, for communication & invoicing:
No comment

Section 4.4.5, to address technical and content issues:
No comment

Section 4.4.6, to address changes to the domain:
No comment

Section 4.4.7, regarding the voluntary provision of administrative and technical contact data:
BC agrees with this section and suggests the following topics for future discussion: Final policy should allow for both request or consent of Registered Name Holder”

Section 4.4.8, to combat abuse and protect intellectual property:
BC agrees with this section and suggests the following topics for future discussion: In the final policy, “Supporting” should be replaced with “Providing” to have parity with other like provisions (e.g., 4.4.9).

Section 4.4.9, to provide LEA access:
No comment

Section 4.4.10, zone-file data:
No comment

Section 4.4.11, to address business or technical failure:
No comment

Section 4.4.12, to facilitate dispute resolution services:
BC agrees with this section and suggests the following topics for future discussion: Not all impacted parties will play a coordinating role in every instance; in some cases, facilitation will be required rather than coordination. Accordingly, the BC suggests replacing “coordinating” with “facilitating”.

Section 4.4.13, to facilitate contractual compliance:
No comment

Section 4.5.1-4.5.5, Rationale for Processing gTLD Registration Data:
No comment

Section 5.1-5.2, Requirements Applicable to Registry Operators and Registrars:
(1) Replace "31 July 2018" with 30 September 2018"; replace "comparable" with "identical". (2) SLAs must conform to the guidance from SSAC 101: "Legitimate users must be able to gain operational access to the registration data that policy says they are authorized to access, and must not be rate-limited unless the user poses a demonstrable threat to a properly resourced system."

Section 5.3-5.5, Requirements Applicable to Registry Operators and Registrars:
BC agrees with this section and suggests the following additional topics for discussion: (1) Process for registrar to determine the adequacy for an international transfer must be explicitly defined. (2) This section must not be over-applied (e.g. to legal persons or in situations unrelated to EEA).

Section 5.6-5.7, Requirements Applicable to Registry Operators and Registrars:
ICANN needs to be allowed full access (not an undefined "reasonable" subset) to RDS data for contractual compliance and for security, stability and resiliency of the DNS (Section 5.7 says "reasonable" and does not cover anything outside of contractual compliance needs). Full access also needs to be clearly defined but shall include Registrant Name, Registrant Organization, Registrant physical address and Registrant email address.

Section 6.1 – 6.3.2, Regarding the requirements for Registry Operators:
Replace "31 July 2018" with 30 September 2018"; replace "comparable" with "identical".

Section 7.1 – 7.1.8, Notices to Registered Name Holders Regarding Data Processing:
BC agrees with this section and suggests the following additional topic for discussion: A similar additional section should be created for resellers; there can be confusion as to who the registrar is when a registrant has registered a domain name with a reseller. As a result, a registrant may not understand why they are receiving this notice from Registrar X when they registered the domain name with Reseller Y. ICANN does not have a direct contractual relationship with the reseller, but the Registrar does and can convey that responsibility.

Section 7.1.9 – 7.1.15, Notices to Registered Name Holders Regarding Data Processing:
No comment

Section 7.2 – 7.2.4, Additional Publication of Registration Data:
(1) The option to consent under Section 7.2.1. should be offered at the same time as the other registrar required notices in 7.1, not at some later undefined date. Replace "As soon as commercially reasonable" with "Along with the notice requirements in 7.1". (2) In 7.2.2, replace "MAY" with "MUST"

Section 7.3-7.4, Uniform Domain Name Dispute Resolution Policy & Transfer Policy:
BC agrees with this section, and suggests the following additional topics for discussion: (1) Lack of Registrant contact data could result in John Doe complaints where a single complainant files a single UDRP with multiple domain names and even multiple registrars. (2) Ability to force the transfer of a domain name without independent confirmation of registrant data seems likely to result in abuse.

Section 8.1 – 8.3, Miscellaneous :
The language is relevant only in regard to the lifecycle of the temp spec (it is severable, has no 3rd party beneficiary, and can be modified by the board). But these conditions may have no applicability to the consensus policy we are planning to create. Once the consensus policy is adopted, the amendments and modifications should run through the normal GNSO policies for updating consensus policies.

Appendix A.1 – A1.2.2, Registration Data Directory Services:
BC agrees with this section and suggests the following topics for future discussion: • Specific durations (e.g. 135 days) should be reviewed later in the process; at this time there is much implementation uncertainty. It may be too early to predict durations which are both expeditious and achievable. • In 1.2.1., "Where search capabilities are permitted and offered" erroneously implies that some Registry Operators and/or Registrars will not provide search capabilities. • In 1.2.2, "(when implemented)" seems confusing and could be replaced with "(as described in 1.2.1)" or similar.

Appendix A.2 – A2.3, Registration Data Directory Services:
BC has the following concerns with this section: • We should not require redaction of data for legal persons or for cases outside of GDPR jurisdiction. • Registrant City and Postal Code should be removed as they are not personally identifiable and are applicable to selection of venue when required for legal action.

Appendix A.2.4 – A2.6, Redacted Fields:
BC has the following concerns with this section: • We should not require redaction of data for legal persons or for cases outside of GDPR jurisdiction. • Registrant City and Postal Code should be removed as they are not personally identifiable and are applicable to selection of venue when required for legal action. • Final policy must accommodate circumstances beyond those supported by an unmonitored web form. Examples include providing a registrant's unique, verified email address (anonymized or other) and registrar being accountable to ensure that mail sent from a web form is received by the registrant and responded to within a defined time interval.

Appendix A.3, Additional Provisions Concerning Processing Personal Data:
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).

Appendix A.4 – A4.2, Access to Non-Public Registration Data:
BC agrees with this section and suggests the following topics for future discussion: • While we anticipate that "reasonable access" will require RDAP and differentiated ("tiered") access, it is the task and responsibility of this policy development panel to work out the definition for reasonableness - panel must delineate processes, timelines, and detailed expected response from Registries and Registrar to reasonable access requests based on legitimate interests as allowed under the GDPR. • As mentioned elsewhere, it may be too soon to determine whether service level assurances ("SLA") such as "within 90 days" are appropriately quick or technically achievable. At this moment, 90 days seems excessively long for most cases. • Regardless of the SLA for access that is ultimately decided, if a Registrar or Registry is presented with an ambiguous situation (where ICANN has not yet published guidance), we believe that there must be an obligation on the Registrar or Registry operator to take immediate action to seek guidance upon receiving a request.

Appendix A.5, Publication of Additional Data Fields:
No comment

Appendix B.1, Supplemental Data Escrow Requirements:
No comment

Appendix B.2, Supplemental Data Escrow Requirements:
No comment

Appendix B.3, Supplemental Data Escrow Requirements:
We may need to define "substantially similar".

Appendix B.4, Supplemental Data Escrow Requirements:
No comment

Appendix C, Data Processing Requirements:
No comment

Appendix C.1 – C.1.6, Data Processing Requirements:
BC can agree with this section if references to "obligations subject to local laws" are changed to instead reference the existing consensus policy and process which already governs conflicts between WhoIs obligations and national data protection laws. The language above creates uncertainty by failing both to reference the existing consensus policy and by leaving applicability of local law subject to each party's interpretations.

Appendix C.2, Data Processing Requirements:
"Except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of Personal Data" should be qualified by the statement "as may be required under GDPR", because not all processing is subject to the balancing test.

Appendix C.3 – C3.1.6, Data Processing Requirements:
BC agrees with this section. We also suggest the following topic for discussion: To ensure that processes successfully improve security, stability and privacy without excessive or unpredictable burden on contracted parties, BC suggests that the panel consider RSEP as an example of a similar policy.

Appendix C.3.2 – C3.5.2, Data Processing Requirements:
BC agrees with this section. We also suggest the following additional topic for discussion: Similar to the language of the RAA, ICANN should develop and propose standard language that could be used as guidance to the contracted parties to meet the transparency requirements in 3.5.1 with regard to the use of WHOIS contact data.

Appendix C.3.8 – C3.10, Data Processing Requirements:
No comment

Appendix D, Uniform Rapid Suspension:
No comment

Appendix E - Uniform Domain Name Dispute Resolution Policy:

No comment

Appendix F - Bulk Registration Data Access to ICANN:

No comment

Appendix G.1 - Supplemental Procedures to the Transfer Policy:

Executing a transfer request at the request of the registrant is consistent with GDPR because it is processing for the performance of the contract. We are concerned about changes which might result in the transfer process becoming less secure. 1.2 also seems to impose redundant process on the Registrant, which is a weaker user experience.

Appendix G.2 - Supplemental Procedures to the Transfer Policy:

No comment

Part 1 – Other – Any Further Input:

Additional suggestions are provided in the comment boxes following each survey question.

Part 2 – Other – Any Further Input:

No comment

Part 3 – Other – Any Further Input:

No comment

Part 4 – Other – Any Further Input:

BC strongly supports the inclusion of each of the issues identified in 1-7 to be addressed in the EPDP, with the exception of the accreditation model, since that work is being pursued on a separate track. As discussed earlier, providing definition to what is meant by "continued [and]public access" falls squarely within this PDP and must be explored

Comments from the IPC

Section 1, Scope:

The IPC is supportive of this section however we believe that allowing ICANN to unilaterally decide when or if requirements should apply is not appropriate for a consensus policy. As such we suggest that the clause "unless ICANN determines in its reasonable discretion that this Temporary Specification SHALL NOT control." be removed in the EPDP policy report.

Section 2, Definitions:

No comment

Section 3, Policy Effective Date:

No comment

Sections 4.1 - 4.2, Lawfulness & Purposes of Processing gTLD Registration Data:

No comment

Sections 4.3, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Section 4.4 - 4.4.1, Lawfulness & Purposes of Processing gTLD Registration Data:
Rationale: Article 2 of GDPR clearly states that several categories/types of processing fall outside its scope and thus are NOT subject to the balancing test of Article 6(1)(f). This includes processing for criminal law enforcement and by competent authorities for safeguarding against and the prevention of threats to public security, which falls outside the scope of the GDPR and instead is subject to Directive (EU) 2016/680. Moreover, Article 6 of the GDPR provides for lawful processing in a number of circumstances as set forth in Article 6(1)(a) - (e), such as processing necessary for the performance of a task carried out in the public interest, that also are NOT subject to the balancing test of "overridden by the interest or fundamental rights" in (f). Finally, Article 6(1) also states that (f) "shall not apply to processing carried out by public authorities in the performance of their tasks." Therefore, Article 4.4 of the Temp Spec is too narrow and does not recognize that there are categories of processing of Personal Data in Registrant Data that are NOT subject to the qualification of "not overridden by the fundamental rights and freedoms of individuals whose Personal Data is included in Registration Data." For processing that is necessary for the purposes of the legitimate interests pursued by the controller or third party, we agree that the balancing test of Article 6(1)(f) applies. However, these legitimate interests under Article 6 pursued by a controller or third party are not defined. We support seeking to identify categories of legitimate interests and purposes that qualify for processing in accordance with Article 6(1)(f) of the GDPR, but caution that the Consensus Policy should not seek to exclusively define such interests by using language such as "only for the following legitimate purposes."

Section 4.4.2, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Section 4.4.3, for contacting registrants:
No comment

Section 4.4.4, for communication & invoicing:
No comment

Section 4.4.5, to address technical and content issues:
No comment

Section 4.4.6, to address changes to the domain:
No comment

Section 4.4.7, regarding the voluntary provision of administrative and technical contact data:
IPC is supportive of this comment however we believe that publication of this data happens at the request *or consent" of the Registered Name Holder. This is consistent with the requirements placed on the Registrar in Section 7.2.4.

Section 4.4.8, to combat abuse and protect intellectual property:
The IPC supports this section however we suggest that in the EPDP report the term "Supporting" be replaced with "Providing" to make it consistent with Section 4.4.9. Note also the comment made to

Question 8. In addition, it may be appropriate to address 4.4.8. and 4.4.9. together because of the overlap of cybercrime and law enforcement.

Section 4.4.9, to provide LEA access:
But please see responses to Question 8 and 15.

Section 4.4.10, zone-file data:
No comment

Section 4.4.11, to address business or technical failure:
No comment

Section 4.4.12, to facilitate dispute resolution services:
The IPC supports this section but believes that more specificity is required in the EPDP report. Specifically the EPDP final report should specify not only coordination but also facilitation of dispute resolution services including providing a forum and creating the necessary processes.

Section 4.4.13, to facilitate contractual compliance:
Under Article 6(1)(b) of the GDPR, processing is lawful when necessary for the performance of a contract to which the data subject is party and it is not subject to the balancing of interests test under Article 6(1)(f).

Section 4.5.1-4.5.5, Rationale for Processing gTLD Registration Data:
IPC is supportive of this section however we believe the EPDP final report should indicate that this applies to Section 6(1)(f) GDPR *where applicable". I.e. "In considering whether Processing of Personal Data contained in Registration Data is consistent with Article 6(1)(f) of the GDPR, *where applicable*, the GDPR requires ICANN to balance the legitimate interests described above with the interests, rights, and freedoms of the affected data subject. Also see our comments to Question 8.

Section 5.1-5.2, Requirements Applicable to Registry Operators and Registrars:
All SLAs associated with RDDS should be measurable, enforceable and be set at levels that do not artificially impede access to properly formed, authenticated and authorized requests to RDS data.

Section 5.3-5.5, Requirements Applicable to Registry Operators and Registrars:
No comment

Section 5.6-5.7, Requirements Applicable to Registry Operators and Registrars:
The IPC supports this section however we believe the use of the term "reasonable access" is vague and ambiguous. As such we believe the EPDP is responsible for developing policy that defines a more definite and concrete definition for the term "reasonable access".

Section 6.1 – 6.3.2, Regarding the requirements for Registry Operators:
We assume that these RDAP related reporting requirements will be in place by the time the Consensus Policy is adopted. We agree that any such requirements should be comparable to existing RDDS related reporting requirements currently in the agreements. We also believe that review and approval of RRA updates is necessary and thus suggest Section 6.3.2 be updated as follows - 6.3.2. Registry Operator MAY amend or restate its Registry-Registrar Agreement to incorporate data Processing terms and conditions (which itself contains EU Model Clauses to govern international data transfers, where

applicable between the respective parties) substantially similar to the requirements provided at <> without any further approval of ICANN, provided that Registry Operator MUST promptly deliver any such amended or restated Registry-Registrar Agreement to ICANN, and subject to ICANN's approval.

Section 7.1 – 7.1.8, Notices to Registered Name Holders Regarding Data Processing:
The IPC supports this section if the following clarifications and corrections are made. In section 7.1.1 the "specific purposes" and in Section 7.1.2 the "intended recipients" must be set and identified via the consensus policy defined by the EPDP team. Section 7.1.7 should apply to legitimate interests (plural) and apply to any lawful process as defined in Article 6 of the GDPR or processing that falls outside of the scope of the GDPR, such as described in Article 2(2)(d) of the GDPR.

Section 7.1.9 – 7.1.15, Notices to Registered Name Holders Regarding Data Processing:
Note however that in Section 7.1.12 the word consent should be a defined term (capital C) in 7.1.12. (e.g. "....relies on Consent…")

Section 7.2 – 7.2.4, Additional Publication of Registration Data:
As a matter of clarification/confirmation, the opportunity for the RNH to Consent to publication of data fields should cover all RDDS data fields supplied by the RNH, and Registrar must publish all the data Consented to by the RNH, in addition to the fields it must otherwise publish even without such Consent. The opportunity to Consent to the publication of additional data fields (e.g. Admin/Tech contacts) should be mandatory, not voluntary/discretionary by the Registrar.

Section 7.3-7.4, Uniform Domain Name Dispute Resolution Policy & Transfer Policy:
No comment

Section 8.1 – 8.3, Miscellaneous :
The IPC supports these sections however we believe that all GAC advice on this subject should be applicable, not just advice from the San Juan Communique.

Appendix A.1 – A1.2.2, Registration Data Directory Services:
IPC is supportive of this section, however we note that the obligation to enable/implement search capabilities are never explicitly required. In order to ensure implementation and support of important search capabilities the EPDP final report must contain a requirement for Registry Operators and Registrars to offer search capabilities in the first place.

Appendix A.2 – A2.3, Registration Data Directory Services:
As detailed in the joint BC and IPC comment on the ICANN Proposed Interim Model for GDPR Compliance, the IPC does not support this section for the following reasons. 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. Supporting References * GDPR, Art. 3 (the regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the Union, or data subjects in the Union). * Hamilton Memo Part 1, Section 3.2.1 - 3.2.2. * Hamilton Memo Part 2, Section 2.1.4 * GAC Feedback on

Proposed Interim Models for Compliance, p. 7, Section IV(D). * Data Protection and Privacy Update – Plans for the New Year ("We've made it a high priority to find a path forward to ensure compliance with the GDPR while maintaining WHOIS to the greatest extent possible."). Second, As ICANN has acknowledged, data of "legal persons," to the extent such data does not reflect "personal data," is not within the scope of the GDPR. We disagree with ICANN's proposal 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, surpassing even the European Commission's own interpretation of the GDPR. It is necessary and feasible for contracted parties to draw the necessary distinction between natural and legal persons. We know this because we have members who do it, at a scale. Ultimately, the distinction must be part of the interim model, and contracted parties' desire to avoid spending resources on GDPR implementation, as our members and companies worldwide are doing, should not, in and of itself, be sufficient justification for over-compliance and departing from the goal of preserving access to WHOIS to the greatest extent possible under the GDPR. Supporting References * GDPR, Art. 1. (the regulation applies to the protection of natural persons with regard to the processing of personal data). * GDPR, Art. 4. (personal data means any information relating to an identified or identifiable natural person). * Hamilton Legal Memo Part 1, Section 3.5.1 ("[D]ata processed through the Whois services will not be covered by the GDPR if it relates solely to a legal person."). * Taylor Wessing Legal Memo, p. 4 section 5. * Wilson Sonsini Legal Memo, p. 6-7 ("[I]f self-identification creates a process by means of which less personal data is included in the registration (e.g., by including only the data of legal persons, which is not considered to be personal data), then it may lower the legal risk."). * GAC Feedback on Proposed Interim Models for Compliance, p. 5 ("Legal persons are not protected by the GDPR. Not displaying their data hinders the purposes of WHOIS without being required by the GDPR. The GDPR only applies to the personal data of natural persons."). * European Commission Letter of February 7, 2018, p. 3 ("The Commission welcomes the distinction between personal data and other data (about legal persons). The GDPR only applies to personal data of natural persons and therefore does not regulate the processing of the data of legal persons (unless such data also relates to an identified or identifiable natural person)." * European Commission Letter of January 29, 2018, p. 3 ("As the GDPR only applies to personal data of natural persons, in a first step, a distinction should be made between data that fall within the scope of the GDPR and other data elements."). * Article 29 Working Party Letter of December 6, 2017, p. 1 (referring to limitations on publication of "personal data of individual domain name holders"). Third, publication of a registrant's email address, as verified by the registrar, along with publication of the other specific registrant data specified in the model, is needed to support public/legitimate interests. The EC's stated interpretation of the GDPR on this point aligns with our position. It reinforces that necessary for performance of a contract, necessary for the public interest, and necessary for legitimate interests are all lawful bases upon which WHOIS data, particularly registrant email addresses, can be publicly available without violating the GDPR. In particular, publishing a registrant's email is critical because it is the primary means of contacting the registrant, which is a fundamental purpose of WHOIS. It is also necessary to carry out myriad legitimate interests. An anonymized email address or web form is unacceptable because it is unlikely to be implemented uniformly and comprehensively by all accredited registrars, and because it would not enable a third party to determine whether the registrant actually received the email pursuant to "bounceback" information. In addition, registrant email is a key means of correlating various domain names registered by a single registrant, even where other data is unavailable or inaccurate (e.g. "Reverse WHOIS"). We would only consider supporting a pseudonymous (not anonymous) email if it is based on validated and verified registrant information (both operationally and syntactically accurate), and is consistent across each underlying unique email address used to register any domain name across all gTLDs. Supporting References * GDPR Art. 5(1)(b) (purposes for the processing of personal data must be specified and explicit). * GDPR, Art. 6. (the lawfulness of processing principles in Art. 6, including: Art. 6(1)(a) (data subject has given consent), Art. (6)(1)(e) (performance of a task carried out in the public interest), and Art. 6((1)f) (processing is necessary for the purpose of the legitimate interests pursued by the controller or by a third party) provide flexibility in publishing data and providing access). Finally, IPC believes that knowing the City of the Registrant is necessary to serve legal process, as such it should not be redacted.

Appendix A.2.4 – A2.6, Redacted Fields:
The IPC does not support this section for the reasons listed in our answer to Question 23. For rational regarding the importance of both the administrative and technical contact data please reference the recent IPC filing made to German Regional Court on July 7, 2016.

Appendix A.3, Additional Provisions Concerning Processing Personal Data:
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.

Appendix A.4 – A4.2, Access to Non-Public Registration Data:
The IPC supports this section and strongly believes that the EPDP is responsible for developing policy that defines the term “reasonable access” which will enable access to non-private whois data as permitted by the GDPR. This includes the concept of “tiered access” and its implementation via the RDAP protocol. Regarding providing reasonable access the IPC believes that 90 days is too long suggests that access should be required as soon as commercial feasible but in no event longer than 15 calendar days, which is consistent with the time period in which registrars must comply with the requirements of the current WHOIS Accuracy Specification under the 2013 RAA, unless the time period for publication or disclosure is otherwise specified by the applicable legislation, court order, or other binding legal authority. The IPC also believes that Section 4.2. is too limited and doesn’t take into account law enforcement and other processing even under GDPR that is NOT subject to the balancing test. At the very minimum, there should be added here a new Section 4.2 that reads as follows and existing Section 4.2 should become 4.3: “Registrar and Registry Operator MUST provide immediate access to Personal Data in Registration Data to competent authorities that seek access to Personal Data 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. Such access shall be granted without any financial charge and the Processing of such Personal Data by such competent authorities is not subject to any restrictions or qualifications that may be set forth in this Temporary Specification and Registrar and Registry Operator may not impose any restrictions or qualifications.” The suggested language follows from Article 2(d) of the GDPR. Access and processing of personal data by law enforcement is not subject to the GDPR and therefore is not subject to any restrictions set forth in the GDPR. ICANN org has utterly failed to recognize this critical point in the Temporary Specification and has arguably violated its Charter and By-laws by so doing.

Appendix A.5, Publication of Additional Data Fields:
No comment

Appendix B.1, Supplemental Data Escrow Requirements:
No comment

Appendix B.2, Supplemental Data Escrow Requirements:
No comment

Appendix B.3, Supplemental Data Escrow Requirements:
No comment

Appendix B.4, Supplemental Data Escrow Requirements:
No comment

Appendix C, Data Processing Requirements:
The IPC supports this section however we note that the above represents some, but not necessarily all, of the bases for processing personal data. In addition we believe that the following update should be made. Replace "...such access will at all times comply with the requirements of the GDPR." with "...such access will comply with the requirements of the GDPR, as applicable".

Appendix C.1 – C.1.6, Data Processing Requirements:
IPC agrees with the bulk of this section but strongly disagrees with the lead in language to this section, which makes the obligations subject to applicable laws. All obligations are subject to applicable laws, but for the sake of certainty, it is important that the obligations be clear and certain, and not subject to any one party's view of what applicable laws require. There is an existing consensus policy and Process to govern conflicts between WHOIS obligations and National Data Protection Laws, and that will govern dealing with any conflict between those laws and such obligations. The language above appears to allow circumvention of that policy and process, and creates uncertainty. Therefore, in Section 1 the phrase "except as required by applicable laws and regulations" should be deleted, as it is unnecessary.

Appendix C.2, Data Processing Requirements:
As we have stated previously (See IPCs answer to Question 8 of Part 1 of the Triage) , this provision wrongfully assumes that data will be processed on the basis of a legitimate interest not overridden by the interests or fundamental rights and freedoms of the data subject. This Article 6 Section 1(f) basis is merely one lawful basis for processing WHOIS data among many potentially lawful bases for processing WHOIS data.

Appendix C.3 – C3.1.6, Data Processing Requirements:
No comment

Appendix C.3.2 – C3.5.2, Data Processing Requirements:
No comment

Appendix C.3.8 – C3.10, Data Processing Requirements:
The IPC agrees with the substance of this question however the following updates should be made. In section 3.8 the term "natural persons" should be replaced by "data subjects" In section 3.10 there is a typo that should be fixed. "compliance with the terms *of* this Section 3.10,

Appendix D, Uniform Rapid Suspension:
The IPC is supportive of this section, subject to the following clarifications. 1.1 - Clarification is needed on "another mechanism to provide the full Registration Data to the Provider as specified by ICANN". Any other mechanism must make full Registration Data available to Complaint so that Complainant has

an opportunity to amend complaint upon obtaining full RDDS data post-filing. “[A]vailable Registration Data should be “full Registration Data”. 2 - Complainant must only be required to insert whatever publicly-available RDDS data exists for the domain name(s) at issue, and must be given the opportunity to file an amended complaint upon obtaining the full RDDS data post-filling.

Appendix E - Uniform Domain Name Dispute Resolution Policy:
The IPC is supportive of this section, subject to the following clarifications. 1.1 - As above, clarification is needed on “another mechanism to provide the full Registration Data to the Provider as specified by ICANN”. Any other mechanism must make full Registration Data available to Complaint so that Complainant has an opportunity to amend complaint upon obtaining full RDDS data post-filing. 1.2 - As above, Complainant must only be required to insert whatever publicly-available RDDS data exists for the domain name(s) at issue, and must be given the opportunity to file an amended complaint upon obtaining the full RDDS data post-filling.

Appendix F - Bulk Registration Data Access to ICANN:
No comment

Appendix G.1 - Supplemental Procedures to the Transfer Policy:
The IPC is supportive of this section, subject to the following clarifications. 1 - We note that RDAP will be in effect and implemented by the time Consensus Policy is adopted. We believe the phrase “to be offered” in Section 1 above should be removed for clarity.

Appendix G.2 - Supplemental Procedures to the Transfer Policy:
The IPC is supportive of this section, subject to further clarification on “best practices”. Will there by agreed-upon mandatory practices?

Part 1 – Other – Any Further Input:
No comment

Part 2 – Other – Any Further Input:
Throughout these polls the text of the Temporary Specification indicate a requirement to adhere to obligations as outlined in a particular Appendix or Section of the Temporary Specification. The IPC believes that these requirements will reference consensus policy of the EPDP team and reference the relevant sections or appendixes of the EPDP final report. Also note that our agreement to Sections that reference certain Appendixes does NOT mean that we agree with all the terms and provisions of the particular Appendix itself.

Part 3 – Other – Any Further Input:
No comment

Part 4 – Other – Any Further Input:
Apart from the issue identified in point #1 of the annex (related to an accreditation model) which IPC supports continued discussion of the important issues enumerated in the Annex by the EPDP team. We understand that the issued address in #1 is subject to the gating questions defined in the charter.

Comments from the GAC

Section 1, Scope:
No comment

Section 2, Definitions:
No comment

Section 3, Policy Effective Date:
No comment

Sections 4.1 - 4.2, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Sections 4.3, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Section 4.4 - 4.4.1, Lawfulness & Purposes of Processing gTLD Registration Data:
Edit: In section 4.4, the second and last sentence "Accordingly, Personal Data included in Registration Data may be Processed on the basis of a legitimate interest not overridden by the fundamental rights and freedoms of individuals whose Personal Data is included in Registration Data, and only for the following legitimate purposes:" Should read: "Accordingly, Personal Data included in Registration Data may be Processed on the basis of a legitimate interest not overridden by the fundamental rights and freedoms of individuals whose Personal Data is included in Registration Data. Accepted legitimate purposes include:" Rationale: current wording suggests an exhaustive list, for a policy for access to Registration data that will last XX years. It can't foresee all legitimate purposes. Additionally, GAC Representatives would like to flag that references to GDPR only in section 4.4 and related subsections may be problematic in regard to other national or regional data protection frameworks. Reference was made to national data protection legislations.

Section 4.4.2, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Section 4.4.3, for contacting registrants:
No comment

Section 4.4.4, for communication & invoicing:
No comment

Section 4.4.5, to address technical and content issues:
No comment

Section 4.4.6, to address changes to the domain:
No comment

Section 4.4.7, regarding the voluntary provision of administrative and technical contact data:

No comment

Section 4.4.8, to combat abuse and protect intellectual property:
GAC Representatives to the EPDP would like to flag this item as not supported but will need more time to propose appropriate language. It is not clear it is formulated as defining a purpose in a way that is consistent with the GDPR.

Section 4.4.9, to provide LEA access:
GAC Representatives to the EPDP would like to flag this item as not supported but will need more time to propose appropriate language. It is not clear it is formulated in a way that defines a purpose in a way that is consistent with the GDPR. The use of the term "Law enforcement" may also need to be modified.

Section 4.4.10, zone-file data:
No comment

Section 4.4.11, to address business or technical failure:
No comment

Section 4.4.12, to facilitate dispute resolution services:
No comment

Section 4.4.13, to facilitate contractual compliance:
No comment

Section 4.5.1-4.5.5, Rationale for Processing gTLD Registration Data:
No comment

Section 5.1-5.2, Requirements Applicable to Registry Operators and Registrars:
Re 5.2 The GAC would like clarification if the SLA have been agreed or what levels have been put in place by ICANN

Section 5.3-5.5, Requirements Applicable to Registry Operators and Registrars:
No comment

Section 5.6-5.7, Requirements Applicable to Registry Operators and Registrars:
No comment

Section 6.1 – 6.3.2, Regarding the requirements for Registry Operators:
At this point in time, GAC Representatives are not in a position to either support or oppose these sections until more information is made available regarding: Section 6.1: Need to know more regarding what is periodic access and to what extent it is absolutely necessary and whether ICANN has some standards/ guidelines for deciding how often is periodic Section 6.2: more information on outcome of negotiations and the scope of the term "reporting requirements" is provided. Additionally, regarding Section 6.3, language needs some modification to allow, "incorporate data processing terms and conditions (which itself contains EU Model clauses to govern international transfers or similar clauses developed by other countries as part of relevant National legislation frameworks while also ensuring compliance to all applicable national laws, where applicable between the respective parties"

Section 7.1 – 7.1.8, Notices to Registered Name Holders Regarding Data Processing:
Section 7.1.7: lack of clarity around the use of the term "legitimate interest" Section 7.1.5: could be modified to read as "…local representative in the jurisdiction such as the European Economic Area, other countries and regions as maybe applicable"

Section 7.1.9 – 7.1.15, Notices to Registered Name Holders Regarding Data Processing:
No comment

Section 7.2 – 7.2.4, Additional Publication of Registration Data:
Section 7.2.1: GAC Representatives request Ry/Rars to provide an actual time frame for providing "the opportunity for the Registered Name Holder to provide its Consent to publish the additional contact information" Section 7.2.2: MAY should read MUST. Rationale: such requirement should apply consistently across all RDS Data (generally subject to MUST).

Section 7.3-7.4, Uniform Domain Name Dispute Resolution Policy & Transfer Policy:
No comment

Section 8.1 – 8.3, Miscellaneous :
No comment

Appendix A.1 – A1.2.2, Registration Data Directory Services:
GAC Representatives to the EPDP would like to flag that consideration of 1.1 to 1.2.1 is contingent on whether the 31 July 2018 deadline has been met or not.

Appendix A.2 – A2.3, Registration Data Directory Services:
Section 2.1: GAC Representatives to the EPDP would like to flag that consideration of this section is still ongoing. Section 2.2: "For fields that section 2.3 and 2.4 of this Appendix requires to be "redacted", Registrar and Registry Operator MUST provide in the value section of the redacted field text substantially similar to the following "REDACTED FOR PRIVACY". Prior to the required date of implementation of RDAP, Registrar and Registry Operator MAY: (i) provide no information in the value section of the redacted field; or (ii) not publish the redacted field." Should read as: "For fields that section 2.3 and 2.4 of this Appendix requires to be "redacted", Registrar and Registry Operator MUST provide in the value section of the redacted field text stating "REDACTED FOR DATA PROTECTION". Rationale: for the sake of greater consistency, the Registrar and Registry Operator should provide the same text in the value fields. Also, "REDACTED FOR DATA PROTECTION" more accurately reflects the reason for redacting (vs "privacy"). Additionally, the GAC would like section 2.2 to include new text that directs WHOIS users to details on how/where to request the non-public (redacted) information.

Appendix A.2.4 – A2.6, Redacted Fields:
Section 2.4.1: GAC Representatives are seeking a unique anonymized email address to identify and reach a given contact across domains and gTLDs, consistent with GAC Advice.

Appendix A.3, Additional Provisions Concerning Processing Personal Data:
GAC Representatives to the EPDP would like to flag that consideration of this section is still ongoing.

Appendix A.4 – A4.2, Access to Non-Public Registration Data:
Section 4 and related subsections: The GAC would like "reasonable access" defined. The GAC would also like these sections to be clarified to make clear that Registrar and Registry Operator responses to

access requests are time bound and that any refusal to provide access be accompanied with a rationale for why.

Appendix A.5, Publication of Additional Data Fields:
No comment

Appendix B.1, Supplemental Data Escrow Requirements:
No comment

Appendix B.2, Supplemental Data Escrow Requirements:
No comment

Appendix B.3, Supplemental Data Escrow Requirements:
No comment

Appendix B.4, Supplemental Data Escrow Requirements:
No comment

Appendix C, Data Processing Requirements:
Suggested edit: in table, line 'Public RDDS/WHOIS', add ‘performance of a contract’ as a legal justification for Public RDDS/WHOIS gTLD processing activity (for all Registrar/Registry/ICANN roles)
Rationale: The public RDDS/WHOIS is a contractual provision and needs to be articulated as such.

Appendix C.1 – C.1.6, Data Processing Requirements:
No comment

Appendix C.2, Data Processing Requirements:
Paragraph does not mention other bases for processing in addition to legal basis (Performance of a Contract, Public Task including maintenance of public order, protection of life). Balancing test in this section (as reflected from Art. 6.1 of the GDPR) does not apply to “processing carried out by public authorities in the performance of their tasks.” Art. 6.1(f)

Appendix C.3 – C3.1.6, Data Processing Requirements:
No comment

Appendix C.3.2 – C3.5.2, Data Processing Requirements:
Section 3.5: before the GAC can confirm whether to support this section or not, it remains to be clarified whether this section is intended to cover disclosure of actual law enforcement requests for personal data.

Appendix C.3.8 – C3.10, Data Processing Requirements:
No comment

Appendix D, Uniform Rapid Suspension:
Despite support in principle, these sections need the following clarifications: Section 1.1: It is not clear what “participate in another mechanism to provide the full Registration Data to the Provider as specified

by ICANN" mean. Section 2: what are the safeguards built in to ensure that this provision of "Doe" complaint is not be abused to get the contact details of the Registered Name Holder.

Appendix E - Uniform Domain Name Dispute Resolution Policy:
Despite support in principle, these sections need the following clarifications: Section 1.1: It is not clear what "participate in another mechanism to provide the full Registration Data to the Provider as specified by ICANN" mean. Section 1.2: what are the safeguards built in to ensure that this provision of "Doe" complaint is not be abused to get the contact details of the Registered Name Holder.

Appendix F - Bulk Registration Data Access to ICANN:
No comment

Appendix G.1 - Supplemental Procedures to the Transfer Policy:
No comment

Appendix G.2 - Supplemental Procedures to the Transfer Policy:
No comment

Part 1 – Other – Any Further Input:
here are descriptive words used throughout the above sections that either don't offer any value or need clarification. One example is the use of 'reliable' in section 4.4.3, may need clarification on its scope of application, and may deserve to be replicated to subsequent sections for consistency (from 4.4.4 to 4.4.6).

Part 2 – Other – Any Further Input:
GAC Representatives would like to flag that as per survey 1 references to GDPR only may be problematic in regard to other national or regional data protection frameworks. Where appropriate language to include national data protection legislations would be helpful. There are descriptive words used throughout the above sections that either don't offer any value or need clarification. Examples are Reasonable access and reasonable notice, under Q5.

Part 3 – Other – Any Further Input:
No comment

Part 4 – Other – Any Further Input:
Addition input will be provided in the GAC Early Input to the EPDP.

Comments from the SSAC

Section 1, Scope:
No comment

Section 2, Definitions:
No comment

Section 3, Policy Effective Date:
n/a

Sections 4.1 - 4.2, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Sections 4.3, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Section 4.4 - 4.4.1, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Section 4.4.2, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Section 4.4.3, for contacting registrants:
No comment

Section 4.4.4, for communication & invoicing:
No comment

Section 4.4.5, to address technical and content issues:
No comment

Section 4.4.6, to address changes to the domain:
No comment

Section 4.4.7, regarding the voluntary provision of administrative and technical contact data:
No comment

Section 4.4.8, to combat abuse and protect intellectual property:
No comment

Section 4.4.9, to provide LEA access:
No comment

Section 4.4.10, zone-file data:
No comment

Section 4.4.11, to address business or technical failure:
No comment

Section 4.4.12, to facilitate dispute resolution services:
No comment

Section 4.4.13, to facilitate contractual compliance:
No comment

Section 4.5.1-4.5.5, Rationale for Processing gTLD Registration Data:
No comment

Section 5.1-5.2, Requirements Applicable to Registry Operators and Registrars:
Yes. We add that rate limiting and whitelisting should be considered when negotiating SLAs. These are discussed in SAC101 here: https://www.icann.org/en/system/sac-101-en.pdf. SSAC has previously asked if this section over-rides the ICANN Procedure for Handling WHOIS Conflicts with Privacy Law. See page 16 of SAC101.

Section 5.3-5.5, Requirements Applicable to Registry Operators and Registrars:
No comment

Section 5.6-5.7, Requirements Applicable to Registry Operators and Registrars:
No comment

Section 6.1 – 6.3.2, Regarding the requirements for Registry Operators:
No comment

Section 7.1 – 7.1.8, Notices to Registered Name Holders Regarding Data Processing:
No comment

Section 7.1.9 – 7.1.15, Notices to Registered Name Holders Regarding Data Processing:
No comment

Section 7.2 – 7.2.4, Additional Publication of Registration Data:
No comment

Section 7.3-7.4, Uniform Domain Name Dispute Resolution Policy & Transfer Policy:
The security of the Transfer Policy is weakened by Appendix G. Specifically, the Gaining Registrar is excused the obligation to obtain authorisation from the registrant. This seems reasonable in light of GDPR redaction. But without this step, authorisation depends on the AuthInfo code, which is not its purpose and is explicitly prohibited in section A.5 of the Transfer Policy. Poor security precautions on AuthInfo codes have led to brute force attacks in the wild. See SAC074 on registrant protection here: https://www.icann.org/en/system/sac-074-en.pdf

Section 8.1 – 8.3, Miscellaneous :
No comment

Appendix A.1 – A1.2.2, Registration Data Directory Services:
No comment

Appendix A.2 – A2.3, Registration Data Directory Services:
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.   2) The remaining thin gTLD registries should be required to move to thick status per the Thick WHOIS Consensus Policy and Board Resolution 2014.02.07.08. This is important to enhance the accuracy of, reliable access to, and uniform handling of Registration Data. See SAC101.   3) Regarding 2.2, operators should be required to always publish the redacted field name itself. Not publishing the redacted field names gives inconsistent output across providers.

Appendix A.2.4 – A2.6, Redacted Fields:

SSAC agrees with 24 with the addition of the following: 1) If the registrar uses a web form, the URL of the registrar's web form must be published in the registrar's WHOIS/RDAP output. 2) If the Registrar or Registry Operator provides a web-based form or a general email address not customized to the domain, the Registry and Registry Operator must: a) provide an email receipt to the user of the web-based form or general email address stating that the email has been received and will be forwarded to the domain contact, and   b) shall document delivery to the domain contact of the communications submitted via the web-based form or general email address. Registrar or Registry Operator shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period shall provide such records to ICANN upon reasonable notice. [This language is based on similar requirements in the RAA regarding abuse complaints.]

Appendix A.3, Additional Provisions Concerning Processing Personal Data:

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.

Appendix A.4 – A4.2, Access to Non-Public Registration Data:

No, because registrars and registry operators must be required to participate in a uniform, coordinated access program that allows predictable tiered access and credentialing. The current language in 26 allows all manner of non-uniform implementations, with no predictability and potentially large operational barriers.

Appendix A.5, Publication of Additional Data Fields:

No comment

Appendix B.1, Supplemental Data Escrow Requirements:

No comment

Appendix B.2, Supplemental Data Escrow Requirements:

No comment

Appendix B.3, Supplemental Data Escrow Requirements:

No comment

Appendix B.4, Supplemental Data Escrow Requirements:

No comment

Appendix C, Data Processing Requirements:

No comment

Appendix C.1 – C.1.6, Data Processing Requirements:

No comment

Appendix C.2, Data Processing Requirements:

No comment

Appendix C.3 – C3.1.6, Data Processing Requirements:

No comment

Appendix C.3.2 – C3.5.2, Data Processing Requirements:

No comment

Appendix C.3.8 – C3.10, Data Processing Requirements:

Technical standards improve over time. This is reflected in the generic wording of GDPR Article 32. The interpretation is too proscriptive, for example 3.8.5 that mandates a particular cryptosystem. This section is weakened in its entirety because 3.8 states "Appropriate ... measures ... MAY include". The word 'SHOULD' would be a better choice, per rfc2119.

Appendix D, Uniform Rapid Suspension:

See response to Q4 below.

Appendix E - Uniform Domain Name Dispute Resolution Policy:

1.2 (Access to Respondent contact) may be a use case for a future differentiated access system. ICANN staff are advised to keep a list of collection purposes that we identify during this PDP, if they're not already doing so. Additionally, the current lack of access may make it harder to consolidate multiple cases involving the same registrant. As a result, dispute resolution caseload may increase. Consolidation is explicitly permitted under UDRP paragraph 4(f), and implicitly in URS.

Appendix F - Bulk Registration Data Access to ICANN:

No comment

Appendix G.1 - Supplemental Procedures to the Transfer Policy:

The security of the Transfer Policy is weakened by Appendix G. Specifically, the Gaining Registrar is excused the obligation to obtain authorisation from the registrant. This seems reasonable in light of GDPR redaction. But without this step, authorisation depends purely on the AuthInfo code, which is not its purpose and is explicitly prohibited in section A.5 of the Transfer Policy. We understand that some registries have unilaterally implemented an optional section of RFC5731, permitting a domain <info> command to be authenticated using the AuthInfo code. This may be a mechanism by which contact info could be provided to the Gaining Registrar, in order to obtain FOA.

Appendix G.2 - Supplemental Procedures to the Transfer Policy:

Agree in general, with some caution on 2.3: 'The term "Publicly accessible Whois" SHALL have the same meaning as "RDDS".' These two terms are not equivalent, because access to RDDS is envisaged as being context dependent. As a result, the availability of a particular dataset (like the contact data referenced in the Transfer Policy) can no longer be taken for granted in a given context.

Part 1 – Other – Any Further Input:

No comment

Part 2 – Other – Any Further Input:
No comment

Part 3 – Other – Any Further Input:
No comment

Part 4 – Other – Any Further Input:
insert comment

Comments from the ALAC

Section 1, Scope:
No comment

Section 2, Definitions:
No comment

Section 3, Policy Effective Date:
No comment

Sections 4.1 - 4.2, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Sections 4.3, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Section 4.4 - 4.4.1, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Section 4.4.2, Lawfulness & Purposes of Processing gTLD Registration Data:
No comment

Section 4.4.3, for contacting registrants:
No comment

Section 4.4.4, for communication & invoicing:
No comment

Section 4.4.5, to address technical and content issues:
No comment

Section 4.4.6, to address changes to the domain:
No comment

Section 4.4.7, regarding the voluntary provision of administrative and technical contact data:
No comment

Section 4.4.8, to combat abuse and protect intellectual property, to provide LEA access
No comment

Section 4.4.9, to provide LEA access:
No comment

Section 4.4.10, zone-file data:
No comment

Section 4.4.11, to address business or technical failure:
No comment

Section 4.4.12, to facilitate dispute resolution services:
No comment

Section 4.4.13, to facilitate contractual compliance:
No comment

Section 4.5.1-4.5.5, Rationale for Processing gTLD Registration Data:
may be waived in cases where illegal activity is being investigated

Section 5.1-5.2, Requirements Applicable to Registry Operators and Registrars:
Support intent, but 5.2 must be updated with respect to service level based on current understanding of agreements reached if any, date and fall-back specification if still applicable.

Section 5.3-5.5, Requirements Applicable to Registry Operators and Registrars:
Agree with intent, but with regard to 5.5, unclear if there are methods that meet Chapter V criteria in all cases.

Section 5.6-5.7, Requirements Applicable to Registry Operators and Registrars:
To the extent possible, more specificity that "reasonable" for access and notice.

Section 6.1 – 6.3.2, Regarding the requirements for Registry Operators:
No comment

Section 7.1 – 7.1.8, Notices to Registered Name Holders Regarding Data Processing:
No comment

Section 7.1.9 – 7.1.15, Notices to Registered Name Holders Regarding Data Processing:
No comment

Section 7.2 – 7.2.4, Additional Publication of Registration Data:
No comment

Section 7.3-7.4, Uniform Domain Name Dispute Resolution Policy & Transfer Policy:

No comment

Section 8.1 – 8.3, Miscellaneous :

8.1 OK; 8.2 is specific to the Temporary Spec and should not be needed. Changes to the resltant EPDP policy will be done by GNSO processes; 8.3 A comparable clause will be needed referencing the policy and not the Temp Spec (Mutatis Mutandis for those legally minded).

Appendix A.1 – A1.2.2, Registration Data Directory Services:

No comment

Appendix A.2 – A2.3, Registration Data Directory Services:

applicable to Natural Persons and NOT Legal Persons

Appendix A.2.4 – A2.6, Redacted Fields:

No comment

Appendix A.3, Additional Provisions Concerning Processing Personal Data:

No comment

Appendix A.4 – A4.2, Access to Non-Public Registration Data:

No comment

Appendix A.5, Publication of Additional Data Fields:

No comment

Appendix B.1, Supplemental Data Escrow Requirements:

No comment

Appendix B.2, Supplemental Data Escrow Requirements:

Agree with intent, but unclear if there are methods that meet Chapter V criteria in all cases.

Appendix B.3, Supplemental Data Escrow Requirements:

No comment

Appendix B.4, Supplemental Data Escrow Requirements:

No comment

Appendix C, Data Processing Requirements:

But this will no doubt change (and be enhanced) as a result of future deliberations.

Appendix C.1 – C.1.6, Data Processing Requirements:

Will no doubt be subject to change as we move forward.

Appendix C.2, Data Processing Requirements:

"Legitimate" may need to be further defined.

Appendix C.3 – C3.1.6, Data Processing Requirements:

3.1.2 may need to have "necessary or appropriate" better defined.   3.1.5 while a good idea, it is not clear how this could be done other than hiring benevolent hackers to test your defenses.

Appendix C.3.2 – C3.5.2, Data Processing Requirements:
No comment

Appendix C.3.8 – C3.10, Data Processing Requirements:
No comment

Appendix D, Uniform Rapid Suspension:
Clarity on the phrase "participate in another mechanism" would be appreciated. Is this just to attempt to get P/P details revealed or is it something else?

Appendix E - Uniform Domain Name Dispute Resolution Policy:
Clarity on the phrase "participate in another mechanism" would be appreciated. Is this just to attempt to get P/P details revealed or is it something else?

Appendix F - Bulk Registration Data Access to ICANN:
No comment

Appendix G.1 - Supplemental Procedures to the Transfer Policy:
1. In section 1, it is not obvious that the simple existence of RDAP will also imply that the Gaining Registrar will have full access to the necessary data.   2. In the absence of RDAP, there does not appear to be adequate protection from domain hijacking (ie the transfer without the approval of the current registrant).

Appendix G.2 - Supplemental Procedures to the Transfer Policy:
No comment

Part 1 – Other – Any Further Input:
No comment

Part 2 – Other – Any Further Input:
No comment

Part 3 – Other – Any Further Input:
No comment

Part 4 – Other – Any Further Input:
No comment