EPDP Team – Temporary Specification Discussion Summary Index

Temp Spec Section	Appendix C	**Date (last update)**	10 September 2018	**Category**	1

Current text

Appendix C: Data Processing Requirements

This Appendix sets out the framework for the Processing and sharing of Registration Data containing Personal Data between the parties as Data Controllers or Data Processors, as identified in the matrix below, and defines the principles and procedures that the parties SHALL adhere to and the responsibilities the parties owe to each other. The parties collectively acknowledge and agree that Processing of Registration Data is to be performed at different stages, or at times even simultaneously, within the Internet's complex environment, by the parties. Thus, this Appendix is required to ensure that where Personal Data may be accessed, such access will at all times comply with the requirements of the GDPR. Unless defined in this Appendix, terms with initial capital letters have the meaning given under the GDPR.

gTLD Processing Activity	**Registrar Role/ Legal Justification**	**Registry Operator Role / Legal Justification**	**ICANN Role / Legal Justification**
Collection of registration data from Registered Name Holder	Controller (Consent and Performance of a Contract)	Controller (Legitimate Interest and Performance of a Contract)	Controller (Legitimate Intere
Transfer of registration data from Registrar to Registry Operator or Registry Operator Back-end Service Provider	Processor (Performance of a Contract)	Controller (Legitimate Interests)	Controller (Legitimate Interests)
Transfer of registration data from Registry Operator to Data Escrow Agent	No role	Processor (Performance of a Contract)	Controller (Legitimate Intere
Transfer of registration data from Registrar to Data Escrow Agent	Processor (Performance of Contract)	No role	Controller (Legitimate Intere
Transfer of registration data to ICANN Contractual Compliance	Processor	Processor	Controller (Legitimate Intere
Transfer of registration data to Emergency Back-end Registry Operator (EBERO)	No role	Processor (Performance of a Contract)	Controller (Legitimate Intere
Public RDDS/WHOIS	Controller (Legitimate Interest)	Controller (Legitimate Interest)	Controller (Legitimate Intere

Disclosure of non-public RDDS/WHOIS to third parties	Controller (Performance of a Contract [can also vary depending upon the requesting party])	Controller (Performance of a Contract [can also vary depending upon the requesting party])	Controller (Performance of a Contract)
Data retention	No role	Processor (Performance of a Contract)	Controller (Performance of a Contract)

1. **Principles for Processing**

Each Controller will observe the following principles to govern its Processing of Personal Data contained in Registration Data, except as required by applicable laws or regulations. Personal Data SHALL:

1.1. only be Processed lawfully, fairly, and in a transparent manner in relation to the Registered Name Holders and other data subjects ("lawfulness, fairness, and transparency");

1.2. be obtained only for specified, explicit, and legitimate purposes (as outlined in Section 4 of this Temporary Specification), and SHALL NOT be further Processed in any manner incompatible with those purposes ("purpose limitation");

1.3. be adequate, relevant, and not excessive in relation to the purposes for which they are Processed ("data minimization");

1.4. be accurate and, if necessary, kept current, as appropriate to the purposes for which they are Processed ("accuracy");

1.5. not be kept in a form that permits identification of the Registered Name Holder and other data subjects for longer than necessary for the permitted purposes ("storage limitation"); and

1.6. be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality").

Each Registrar and Registry Operator SHALL be responsible for, and be able to demonstrate compliance with principles (1.1) to (1.6) ("accountability"). The Registrar or Registry Operator SHALL inform ICANN immediately if such Registrar or Registry

Operator (i) cannot abide by the Processing principles outlined in Section 1 of this Appendix, or (ii) receives a complaint by a Registered Name Holder or other data subject that the Registrar or Registry Operator has failed to abide by such principles.

2. **Lawfulness of Processing**

For Personal Data Processed in connection with the Registration Data Directory Services, such Processing will take place on the basis of a legitimate interests of the Controller or of the third party or parties to whom the Personal Data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of Personal Data, in particular where the data subject is a child. For other Personal Data collected for other purposes, such Personal Data SHALL NOT be Processed unless a legal basis specified under Article 6(1) GDPR applies.

3. **Specific Controller Processing requirements**

In addition to the general principles and requirements for lawful Processing, each Controller SHALL comply with the following specific requirements:

3.1. **Implementing appropriate measures.** Implementing appropriate technical and organizational measures to ensure and to be able to demonstrate the Processing is performed in compliance with the GDPR, such as appropriate data protection policies, approved code of conducts or approved certification mechanisms. Such measures SHALL be reviewed regularly and updated when necessary by the Controller. The parties acknowledge and agree that they are responsible for maintaining appropriate organizational and security measures to protect such Personal Data shared between the parties in accordance with applicable laws. Appropriate organizational and security measures are further enumerated in Section 3.8 of this Appendix, and generally MUST include:

3.1.1. Measures to ensure that only authorized individuals for the purposes of this Appendix can access the Personal Data;

3.1.2. The pseudonymisation and encryption of the Personal Data, where necessary or appropriate;

3.1.3. The ability to ensure continued confidentiality, integrity, availability and resilience of its processing systems and services;

3.1.4. The ability to restore the availability and access to Personal Data in a timely manner;

	3.1.5. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Personal Data; and 3.1.6. Measures to identify vulnerabilities with regard to the processing of Personal Data in its systems; 3.2. **Engaging only selected Processors.** Engaging only selected Processors and implementing a contract with each Processor that sets out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of data subjects and the obligations and rights of the Controller. The engagement of Processor must comply with Article 28 of the GDPR; 3.3. **Designating a Data Protection Officer.** Designating a "Data Protection Officer" where required by Article 37 of the GDPR or Member State national data protection law; 3.4. **Maintaining a record of Processing.** Maintaining a record of the Processing activities under the Controller's responsibility in accordance with Article 30 of the GDPR; 3.5. **Providing transparent information.** Taking appropriate measures to provide any information referred to in Articles 13 and 14 of the GDPR and any communication under Articles 15 to 22 and 34 of the GDPR relating to Processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, which SHALL specifically include the following obligations: 3.5.1. The parties SHALL ensure that their privacy notices are clear and provide sufficient information to Data Subjects in order for them to understand what of their Personal Data the Parties are sharing, the circumstances in which it will be shared, the purposes for the data sharing and either the identity with whom the data is shared or a description of the type of organization that will receive the Personal Data; 3.5.2. The parties undertake to inform Data Subjects of the purposes for which it will process their Personal Data and provide all of the information that it must provide in accordance with applicable laws, to ensure that the Data Subjects understand how their Personal Data will be processed by the Controller. 3.6. **Facilitating of the exercise of data subject rights.** Facilitating the exercise of data subject rights under Articles 15 to 22 of the GDPR. In the cases referred to in Article 11(2) of the GDPR, the Controller SHALL NOT refuse to act on the request of the

data subject for exercising his or her rights under Articles 15 to 22 of the GDPR, unless the Controller demonstrates that it is not in a position to identify the data subject;

3.7. **Implementing measures for data protection by design and by default.** Implementing appropriate technical and organizational measures, both at the time of the determination of the means for Processing and at the time of the Processing itself, which are designed to implement data protection principles, in an effective manner and to integrate the necessary safeguards into the Processing in order to meet the requirements of the GDPR and to protect the rights of data subjects. Implementing appropriate technical and organizational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are Processed.

3.8. **Implementing appropriate security measures.** Implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risk of data Processing, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. Appropriate technical and organizational measures to protect the Personal Data shared against unauthorized or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure, MAY include, but not limited to:

3.8.1. Ensuring IT equipment, including portable equipment is kept in lockable areas when unattended;

3.8.2. Not leaving portable equipment containing the Personal Data unattended;

3.8.3. Ensuring use of appropriate secure passwords for logging into systems or databases containing Personal Data shared between the parties;

3.8.4. Ensuring that all IT equipment is protected by antivirus software, firewalls, passwords and suitable encryption devices;

3.8.5. Using industry standard 256-bit AES encryption or suitable equivalent where necessary or appropriate;

3.8.6. Limiting access to relevant databases and systems to those of its officers, staff, agents, vendors and sub-contractors who need to have access to the Personal Data, and ensuring that passwords are changed and updated regularly to prevent inappropriate access when individuals are no longer engaged by the party;

3.8.7. Conducting regular threat assessment or penetration testing on systems; and

	3.8.8. Ensuring all authorized individuals handling Personal Data have been made aware of their responsibilities with regards to handling of Personal Data. 3.9. **Developing procedures for breach notification.** Developing procedures for breach notification to ensure compliance with the obligations pursuant to Articles 33-34 of the GDPR. Any notifications provided in connection with Articles 33-34 of the GDPR SHALL also be provided to ICANN. Where a party is not the Data Controller, it must communicate any data security breach immediately after discovery thereof and will provide immediate feedback about any impact this incident may/will have on the Controller and any Personal Data shared with the Controller. Such notification will be provided as promptly as possible. 3.10. **Observing conditions for international data transfers.** Observing conditions for international data transfers so that any transfer of Personal Data which are undergoing Processing or are intended for Processing after transfer to a third country or to an international organization SHALL take place only if the conditions laid down in Chapter V of the GDPR are complied with, including for onward transfers of Personal Data from the third country or an international organization to another third country or to another international organization. A party may only transfer Registration Data including Personal Data relating to EU individuals to outside of the EU (or if such Personal Data is already outside of the EU, to any third party also outside the EU), in compliance with the terms this Section 3.10, and the requirements of applicable laws. 3.11. **Cooperating with Supervisory Authorities.** Cooperating with Supervisory Authorities, on request, in the performance of their tasks.		
	Support as is	**No strong Opinion**	**Does not support as is**
Preamble	55.56%	11.11%	33.33%
1-1.6	44.44%	0%	55.56%
2	33.33%	0%	66.66%
3-3.1.6	77.77%	0%	22.22%
3.2-3.7	55.56%	0%	44.44%
3.8-3.11	55.56%	11.11%	33.33%
Dependency on other sections of the Temp Spec	Section 4.4		

Related Charter Question(s)	Part 1: Purposes for Processing Registration Data a) Purposes outlined in Sec. 4.4.1-4.4.13 of the Temporary Specification: a1) Are the purposes enumerated in the Temporary Specification valid and legitimate? a2) Do those purposes have a corresponding legal basis? a3) Should any of the purposes be eliminated or adjusted? a4) Should any purposes be added? h) Applicability of Data Processing Requirements h1) Should Registry Operators and Registrars ("Contracted Parties") be permitted or required to differentiate between registrants on a geographic basis? h2) Is there a legal basis for Contracted Parties to differentiate between registrants on a geographic basis? h3) Should Contracted Parties be allowed or required to treat legal and natural persons differently, and what mechanism is needed to ensure reliable determination of status? h4) Is there a legal basis for Contracted Parties to treat legal and natural persons differently? h5) What are the risks associated with differentiation of registrant status as legal or natural persons across multiple jurisdictions? (See EDPB letter of 5 July 2018)
Proposed Response to Charter Question(s)	
DPA / EDPB Guidance	

Proposed Changes / Rationale for Change Preamble	
RySG	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.
RrSG	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.
IPC	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".
BC	
ISPCP	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.
NCSG	The NCSG has no strong opinion on this language; however we do have some concerns regarding the contents of Appendix C.
ALAC	But this will no doubt change (and be enhanced) as a result of future deliberations.
GAC	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.
SSAC	
High level summary of the deliberations and/or recommendation(s)	

Proposed Changes / Rationale for Change 1 – 1.6 Principles for Processing	
RySG	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.
RrSG	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.
IPC	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.
BC	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.
ISPCP	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.
NCSG	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.

ALAC	Will no doubt be subject to change as we move forward.
GAC	
SSAC	
High level summary of the deliberations and/or recommendation(s)	

Proposed Changes / Rationale for Change 2 Lawfulness of Processing	
RySG	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.
RrSG	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?
IPC	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.
BC	"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.
ISPCP	As above, basic principles of GDPR (Art. 32) are cited or paraphrased. That is of limited value.

NCSG	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.
ALAC	"Legitimate" may need to be further defined.
GAC	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)
SSAC	
High level summary of the deliberations and/or recommendation(s)	

Proposed Changes / Rationale for Change 3-3.1.6 Specific Controller Processing requirements	
RySG	The concepts here are all standard with regard to security requirements of the GDPR (resiliency and reliability of systems, etc) 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).
RrSG	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.
IPC	
BC	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.
ISPCP	As above, basic principles of GDPR (Art. 32) are cited or paraphrased. That is of limited value.

	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.
NCSG	
ALAC	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.
GAC	
SSAC	
High level summary of the deliberations and/or recommendation(s)	

Proposed Changes / Rationale for Change 3.2-3.7 Specific Controller Processing requirements	
RySG	The concepts here are all standard with regard to security requirements of the GDPR (resiliency and reliability of systems, etc) 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 agrement 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).
RrSG	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.
IPC	
BC	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.
ISPCP	As above, basic principles of GDPR (Art. 32) are cited or paraphrased. That is of limited value.

	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.
NCSG	The NCSG believes that more detail is required in this section in terms of how privacy-by-design ought to be implemented.
ALAC	
GAC	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.
SSAC	
High level summary of the deliberations and/or recommendation(s)	

Proposed Changes / Rationale for Change 3.8-3.11 Specific Controller Processing requirements	
RySG	The concepts here are all standard with regard to security requirements of the GDPR (resiliency and reliability of systems, etc) 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.
RrSG	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.
IPC	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,
BC	
ISPCP	As above, basic principles of GDPR (Art. 32) are cited or paraphrased. That is of limited value. 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.
NCSG	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.
ALAC	
GAC	
SSAC	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.
High level summary of the deliberations and/or recommendation(s)	

Early Input Feedback	**IPC**: Appendix C.1 of the Temporary Specification lists several principles to govern the processing of personal data in the WHOIS system, “except as required by applicable laws or regulations.” We note that all obligations are subject to applicable laws, therefore, 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 policy and process to govern conflicts between WHOIS obligations and National Data Protection Laws, that must govern any conflict between those laws and such obligations. The language above appears to allow circumvention of that policy and process and creates uncertainty. Because of this uncertainty, the IPC recommends that equivalent language in the EPDP final Consensus Policy should be modified to ensure certainty. For example, the phrase “except as required by applicable laws

	and regulations" should be deleted, as it is unnecessary and creates confusion as to the applicability of the WHOIS Conflicts procedure. **GAC:** Introduction: Suggested edit: 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. 2: Paragraph does not mention legal basis for processing in addition to legitimate interest (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) 3.5: Section 3.5: before the GAC can confirm whether to support this sections or not, it remains to be clarified whether this section is intended to cover disclosure of actual law enforcement requests for personal data. --- **RySG**: The RySG considers certain issues such as SLAs, reporting requirements, operationalizing data escrow requirements, and the specific language of contractual provisions to be contractual matters that should not be in the Temporary Specification and that the WG should exclude from its policy recommendations. (§§ 5.2, 5.3, 5.7, 6.3; App. B; App. C). Appendix C should be removed from the scope of the EPDP WG's consideration. Appendix C contains terms intended to be contractual in nature, outside the Picket Fence, and not appropriate for consensus policy. The WG should recommend that ICANN must engage with the Contracted Parties to put in place the legally required instruments (such as a Data Processing Agreement (Art. 28) or Joint Controller Agreement (Art. 26), as appropriate) without further delay. The WG should further recommend that such a review of contracts (for the purposes of data protection arrangements), must extend to those other service providers, which are equally essential to the DNS ecosystem, including, but not limited to EBERO providers, Data Escrow agents and the RPM, UDRP and URS providers. Contracted Parties have provided a full analysis and comment regarding Appendix C (see here for further details)

Proposal from RySG
The Registries Stakeholder Group ("RySG") proposes removal of Appendix C of the Temporary Specification from the scope of the EPDP's consideration. In our view ICANN drafted Appendix C as an emergency substitute for the GDPR mandated data protection agreements between ICANN and Contracted Parties. Accordingly, ICANN and the Contracted Parties should address the subject matter of Appendix C via separate contractual negotiations. From the point of view of the Contracted Parties, one of the most important elements of pre-GDPR preparation was the execution of appropriate data protection agreements between ICANN and the Contracted Parties (e.g. Data Processing Agreement Joint Controller Agreement, Industry Code of Conduct). GDPR explicitly requires written agreements to set out the relationship obligations and instructions for data processing between parties. Unfortunately, ICANN's approach to implementing GDPR compliance did not include a contractual amendment process to develop and execute these agreements. Instead, the principles normally found in these agreements are included in Appendix C. Despite their presence in the Temporary Specification, these issues remain contractual in nature and ICANN should handle them in a bilateral manner with Contracted Parties. Moreover, as a contractual matter, these issues are neither appropriate for inclusion in a GNSO policy, nor are they within the scope of the EPDP. As discussed on a number of occasions thus far in the EPDP, contractual agreements are outside of the Picket Fence and are not appropriate for consensus policy. However, the RySG does recognize that determinations by the EPDP regarding key elements of the Temporary Specification (e.g. identifying data elements, roles and responsibilities of parties, purposes for processing) will inform the development of appropriate agreements between ICANN and Contracted Parties. These decisions may also help determine whether a Joint Controller Agreement, Code of Conduct, or Data Processing Agreement is the most appropriate format given the roles and responsibilities identified by the EPDP. Further, the RySG does not believe that the removal of Appendix C from the scope of the EPDP in any way diminishes discussions regarding third-party access to registration data. The reference to "Disclosure of non-public RDDS/WHOIS to third parties" in the Appendix C table is not an independent source of a right of access for third parties. The table is only a reflection of the roles, rights, and obligations of ICANN and Contracted Parties found elsewhere in the Temporary Specification and other applicable consensus policies. Those other sources (e.g. Appendix A, Section 4) are the more appropriate places to discuss and determine the scope of third party access and are not impacted by the removal of Appendix C from discussion. For the reasons stated above, the RySG proposes that the EPDP adopt, as a formal recommendation to the GNSO, that ICANN and Contracted Parties address Appendix C outside of the EPDP process. This approach allows ICANN and Contracted Parties to benefit from the decisions and policy developed by the EPDP while still ensuring that the appropriate contractual partners develop the agreements.

Proposal from Margie Milam

Rationale for Retention of Appendix C
 	
In general, Appendix C contains a commitment to processing personal data in accordance with the principles laid out in the Appendix that are not included elsewhere in the Temporary Specification. Some of these sections provide the specificity needed to apply GDPR to the different activities identified in the matrix. It's not sufficient to say that the Appendix is not needed because the controllers/processors will simply comply with GDPR, because there are different interpretations of how GDPR applies to RDDS/WHOIS data. Keeping Appendix C will ensure that there is transparency and accountability for the broader ICANN community, as well as the registrants, regarding what is expected by controllers, processors, and third party accessors with legitimate purposes.
 	
Sections to Delete or Rewrite to be More Specific:
I agree with James that some sections in Appendix C lack sufficient detail for how GDPR applies to RDDS/WHOIS, and seem to be merely recitals of GDPR. These could be deleted or be rewritten to be more specific. Examples are: Sections 3.1.1-3.1.6, 3.2, 3.3, 3.6, 3.7., 3.10 & 3.11.
 	
Sections to Retain:
• Section 1
• Section 2 – Replace it with something like – "processing will take place in accordance with the purposes described in Section 4 of the Temp. Spec."
• Section 3 –
    o 3.1 & 3.9: Replace references to GDPR with "applicable data protection law"
    o Section 3.4 – ICANN should clarify what types of records should be maintained with regard to RDDS/WHOIS records
    o Section 3.5 – Replace with a commitment to provide a standard notice to be developed by ICANN that is concise, transparent, plain language, etc. for RDDS/WHOIS.
• Section 3.8 – Delete the specific operational details in 3.8.1, but retain the high level principles in the first few sentences, ending the paragraph with "….alteration or disclosure." In the implementation stage, ICANN should identify specific operational requirements appropriate for the RDDS/WHOIS data, and include them in the applicable contract.
 	
Additional Terms for Appendix C: There should be standard terms applicable to the Third parties who access non-public data, similar to requirements in Section 1. Just like RAA Section 3.7.7's requirements for registration agreements with registrants, standard access agreement terms should be specified in the RAA to apply to the 3rd parties who access the data (specify their legitimate purposes for accessing the data, agree that they won't use that data in a manner incompatible with those purposes, etc.). Without standard T&Cs, each controller/processer could come up with its own access agreement that is either too lax or too onerous

Proposed modification of text (if appropriate)
[Include proposed modifications to the text, if applicable]
Level of Support
[Indicate level of support for proposed modification, per designations in the charter]