Registries Stakeholder Group Early Input on the Temporary Specification

The Registries Stakeholder Group's ("RySG") goal in the EPDP WG is to participate actively and in good faith towards a consensus policy that addresses the questions set forth in the EPDP Charter. The RySG believes that any consensus policy developed by the EPDP must provide a clear path for compliance with the GDPR, be commercially reasonable and implementable, takes into account our differing business models, and does not inhibit innovation.

Key Themes

Commitment to the EPDP's Success. The RySG firmly believes that the EPDP and its task are of vital importance to the registration data system, but especially to the contracted parties, who will bear the majority of the implementation burden. We are tasked with creating a legally sound policy before the Temporary Specification expires on 25 May 2019. In the absence of consensus, contracted parties may find it necessary to implement differing policies to comply with their respective local, national, and supranational legal obligations, all of which supersede any ICANN contract. This scenario is not in the ICANN community's interest. The RySG wants to avoid this situation, and is therefore committed to the EPDP's success. We strongly urge all stakeholders to focus on the achievement of the shared goals, as stated, above other all other considerations.

Approach. It is important to assess the concepts – not the specific language – of the Temporary Specification. The policy recommendations that the Working Group ("WG") will develop must be evergreen and flexible, which cannot be achieved by merely redlining the Temporary Specification. We also caution against over-reliance on specific references to the GDPR, as the ultimate policy should reflect general data protection principles.

- Data Impact Assessment Approach. The RySG recognizes the difficulties inherent in attempting to base reliable policy on a principle-based legislative effort. However, the WG cannot conclude that its policy recommendations are necessarily "legal" or "compliant" unless and until these recommendations are tested by a relevant court or an applicable Data Protection Authority. The WG should to engage in a transparent and uniform assessment approach by assessing each recommendation against fundamental principles of Data Protection such as data minimization, necessity, privacy by design, and default and proportionality. The WG should consider each of the required elements of GDPR Article 35 as a guide to assessing the privacy impacts in completing its tasks. The WG should begin with the fundamentals – the relevant parties, their roles, data flows, and associated data elements. This approach enables the WG to determine the underlying purposes, which are the key foundation for the remaining policy, contract, and data access discussions.

European Data Protection Board (EDPB) Guidance. It is indisputable that the EDPB's guidance will be invaluable to the WG's work and will lend the much sought-after stability and legitimacy to its recommendations. The WG must not, however, seek any input from the EDPB unless the WG is capable of providing the detail and evidence of its deliberations necessary for a request for EDPB consideration. GDPR Article 36 contains the requirements for an EDPB consultation. At a minimum, the WG deliberations should be capable of meeting the requirements outlined in GDPR Article 35. The RySG believes that this approach is not overly reliant on GDPR, but is universally applicable, and specifically requesting EPDB consideration will bring that stability the industry is pursuing. In addition, the WG should take into account the past written guidance from the EDPB and Article 29 relevant to its work. The EDPB has issued specific guidance regarding processing of personal data for WHOIS or equivalent systems. The RySG believes the specific published guidance of the WP29 on key issues such as 'Legitimate Interests of the Data Controller', [1] and 'Opinion 03/2013 on Purpose limitation',[2] are persuasive authority in the WG's deliberations.

Threshold Issues. As a prerequisite to its further work, the WG must specifically deliberate on if the purposes and legal bases set forth in the Temporary Specification are appropriate and, if so, if the identified data elements remain justifiable and necessary to achieve the agreed-upon purposes. (If the WG determines the purposes and legal bases are not appropriate, it must identify new ones before assessing the identified data elements.) The WG must also clearly define the roles of ICANN, Registry Operators, and Registrars throughout the lifecycle of a domain name registration. (§§4, 5.5)

Contractual Matters Beyond Scope of Consensus Policy and the EPDP (Picket Fence Issues). 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)

Early Recommendations. Given the EPDP's expedited nature, the WG should consider, whenever possible, drafting and submitting early recommendations where the WG concludes that such recommendations are intrinsic to the intended policy outcomes, may require time to implement, and deferring such recommendations to the WG's final report may cause long implementation delays. The WG's first such early recommendation should be that ICANN initiate now data processing agreement negotiations with third-party providers of UDRP and URS dispute resolution services, EBERO, and data escrow agent services.

Unnecessary Provisions. In some cases, Temporary Specification provisions are unnecessary because an existing agreement addresses the issue. (App. A, § 1.2)

Pending Litigation and/or EPDB Advice. The outcome of pending litigation and/or EPDB advice could impact the subject matter of some Temporary Specification provisions. (§4; App. A, § 2.4)

[1] http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

[2] http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Defer Access Discussions. The WG should defer access discussions until after it has completed its deliberations on other Temporary Specification elements and answered the gating questions set forth in the WG's charter. (App. A, § 4) The RYSG believes that the parties involved in the processing of data to effect domain name registrations are in the unique position of defining purpose. The EDPB has stated that third party purposes (i.e., access) should not be included in that effort. The RYSG looks forward to dedicating time to discussing a more standard and predictable approach to access at a later stage within the EPDP.

Realistic Technical Expectations: The WG policy recommendations must set expectations that take into account current policy and technology limitations, the state of the art, and implementation costs, and limit its recommendations to measures which are appropriate to the nature of the data being processed. The WG should not issue policy recommendations that are impossible or effectively impossible to implement for technology and financial reasons. The WG must ensure that its policy recommendations undergo formal and reasonable technical implementation review before ICANN Board consideration.

Comments on Specific Sections

Data Processing Requirements. 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 attached).

Consent Mechanisms. There are no established and widely used mechanisms for obtaining or tracking consent by registrants to publication of certain personal data by Registry Operators and Registrars, or for potentially passing that consent from Registrars to Registry Operators or vice versa in a manner consistent with the strict requirements of GDPR. (§7.2.1-.4; App. A., §§ 2.3-4)

Uniform Rapid Suspension. The RySG does not have concerns with the text of Appendix D. However, the RySG has asked ICANN to provide the EPDP WG with the opportunity to review ICANN's agreements with the URS Providers to confirm that these agreements contain the provisions for legal guarantees, protection for transfer outside the EU, and disclosure to third parties, inter alia, required under GDPR. (§5.6; App. D)

Uniform Domain Name Dispute Resolution Policy. The RySG does not have concerns with the text of Appendix E. However, the RySG has asked ICANN to provide the EPDP WG with the opportunity to review ICANN's agreements with the UDRP Providers to confirm that these agreements contain the provisions for legal guarantees, protection for transfer outside the EU, and disclosure to third parties, inter alia, required under GDPR. (§7.3; App. E)

Data Escrow. Differences in escrow agreements, especially across legacy and new gTLDs, make it difficult to operationalize certain Temporary Specification requirements. Also, ICANN is currently proposing data processing terms between ICANN and the data escrow agent. (§5.3; App. B.)

Registration Data Access Protocol. RDAP developments are likely to supersede or otherwise impact the specific requirements in the Temporary Specification. (§5.2; §6.2; App. A, §§ 1.1, 2.2)

Supplemental Procedures to the Transfer Policy. Appendix G is intended as a temporary, stop-gap measure. Because the ICANN community is already working to replace/modify the transfer policy, the RySG believes Appendix G's content is more appropriately handled through those efforts. (App. G)

Support As Is. The RySG supports as is the following sections of the Temporary Specification: § 6.1; App. A, §3; and App. F.

Recommendation for Removal of Appendix C from EPDP Scope

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.

Annex 1: Temporary Specification, Appendix C

A review of Appendix C reveals that the terms mirror the data protection principles and requirements found in Article 28 of the GDPR, which are required, per Article 28(3) to be included in a "contract or other legal act under Union or Member State law." The comments below illustrate these similarities:

Appendix C Preamble: 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.

RySG Response: This language is a hybrid approach combining elements of both Article 28 (1), noting that the data processor must only process data as per the written instructions of the Data Controller, and Article 26 requiring a written agreement between Joint Controllers. This hybrid approach is unlikely to pass muster with the Data Protection Authorities, as it does not meet the clear thresholds as outlined in the respective articles of the GDPR. These requirements are better addressed via contractual arrangements between ICANN and Contracted Parties.

Appendix C Preamble: 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.

RySG Response: The intention of this closing section of the preamble is an acceptance that the DNS does not adhere to standard data processing flows and that a concerted effort is required to map the unique processes within the DNS industry (e.g. as might be identified as part of Article 40 Code of Conduct). The RySG position is that the EPDP should recommend adoption of a Code of Conduct to the GNSO as a future policy development. However, creation of such a Code of Conduct exceeds the scope of the EPDP.

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 Interest)
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 Interest)
Transfer of registration data from Registrar to Data Escrow Agent	Processor (Performance of Contract)	No role	Controller (Legitimate Interest)
Transfer of registration data to ICANN Contractual Compliance	Processor	Processor	Controller (Legitimate Interest)

Transfer of registration data to Emergency Back-end Registry Operator (EBERO)	No role	Processor (Performance of a Contract)	Controller (Legitimate Interest)
Public RDDS/WHOIS	Controller (Legitimate Interest)	Controller (Legitimate Interest)	Controller (Legitimate Interest)
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)

RySG Response: The RySG does not believe this chart is comprehensive and the EPDP should not include this section in a future consensus policy. As stated above, we believe that the data flow analysis conducted under the purposes for processing evaluation will replace this chart.

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:

RySG Response: The data protection principles outlined in Article 5 of GDPR form the fundamental basis for any compliant data processing model. RySG believes that a consensus policy should build on these principles rather than explicitly (and redundantly) include them in the policy. Moreover, any actions to develop and implement the appropriate agreements between ICANN and Contracted Parties should also build on these same principles.

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");

RySG Response: Section 1.1 repeats a high level GDPR principle for data processing contained in Article 5(1)(a). The inclusion is therefore in anticipated compliance with the requirements of Article 28(1), whereby a processor is required to "meet the requirements of [the GDPR]."

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");

RySG Response: Section 1.2 repeats a high level GDPR principle for data processing contained in Article 5(1)(b). The inclusion is therefore in anticipated compliance with the requirements of Article 28(1), whereby a processor is required to "meet the requirements of [the GDPR]."

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

RySG Response: Section 1.3 repeats a high level GDPR principle for data processing contained in Article 5(1)(c). The inclusion is therefore in anticipated compliance with the requirements of Article 28(1), whereby a processor is required to "meet the requirements of [the GDPR]."

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

RySG Response: Section 1.4 repeats a high level GDPR principle for data processing contained in Article 5(1)(d). The inclusion is therefore in anticipated compliance with the requirements of Article 28(1), whereby a processor is required to “meet the requirements of [the GDPR].”

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

RySG Response: Section 1.5 repeats a high level GDPR principle for data processing contained in Article 5(1)(e). The inclusion is therefore in anticipated compliance with the requirements of Article 28(1), whereby a processor is required to “meet the requirements of [the GDPR].”

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").

RySG Response: Section 1.6 repeats a high level GDPR principle for data processing contained in Article 5(1)(f). The inclusion is therefore in anticipated compliance with the requirements of Article 28(1), whereby a processor is required to “meet the requirements of [the GDPR].”

Each Registrar and Registry Operator SHALL be responsible for, and be able to demonstrate compliance with principles (1.1) to (1.6) ("accountability").

RySG Response: This section repeats a high level GDPR principle for data processing contained in Article 5(2). The inclusion is therefore in anticipated compliance with the requirements of Article 28(1), whereby a processor is required to “meet the requirements of [the GDPR].”

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.

RySG Response: This language is another "instruction" to a processor regarding required notifications of events that may significantly impact the parties. This language is more correctly included in an agreement between ICANN and Contracted Parties and is inappropriate for the inclusion in the scope of the EPDP.

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.

RySG Response: This section repeats a high level GDPR principle for data processing contained in Article 6(1)(f) and Article 8. The inclusion is therefore in anticipated compliance with the requirements of Article 28(1), whereby a processor is required to "meet the requirements of [the GDPR]."

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;

RySG Response: Section 3.1 repeats a high level GDPR principle for data processing contained in Article 5(1)(f) and provides the specific detail of Article 32. The inclusion is therefore in anticipated compliance with the requirements of Article 28(3)(c), whereby a processor is required, per the required written agreement, to "take all measures required pursuant to Article 32"."

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;

RySG Response: As specifically noted in Section 3.2, this repeats a high level GDPR principle for data processing contained in Article 28. The inclusion is

therefore in anticipated compliance with the requirements of Article 28(2), whereby a processor is required, per the required written agreement, "not engage another processor without prior specific or general written authorisation of the controller" etc.

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;

RySG Response: Section 3.3 repeats a high level GDPR principle for data processing contained in Article 37. The inclusion is therefore in anticipated compliance with the requirements of Article 28(1), whereby a processor is required to "meet the requirements of [the GDPR]."

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;

RySG Response: Section 3.4 repeats a high level GDPR principle for data processing contained in Article 30. The inclusion is therefore in anticipated compliance with the requirements of Article 28(1), whereby a processor is required to "meet the requirements 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.

RySG Response: Section 3.5 repeats a high level GDPR principle for data processing contained in Articles 13 and 14. The inclusion is therefore in anticipated compliance with the requirements of Article 28(1), whereby a processor is required to "meet the requirements of [the GDPR]."

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;

RySG Response: Section 3.6 repeats a high level GDPR principle for data processing contained in Articles 15-22. The inclusion is therefore in anticipated compliance with the requirements of Article 28(3)(e), whereby a processor is required, per the required written agreement to assist in the fulfillment of the controller's obligations to " respond to requests for exercising the data subject's rights laid down in Chapter III."

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.

RySG Response: Section 3.7 repeats a high level GDPR principle for data processing contained in Article 28(1) to ensure that a processor meets the requirements of GDPR, specifically those as set in Article 25 .

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.

RySG Response: Section 3.8 (including 3.8.1 - 3.8.8) repeats a high level GDPR principle for data processing contained in Article 32. The inclusion is therefore in

anticipated compliance with the requirements of Article 28(3)(c), whereby a processor is required to "take[] all measures required pursuant to Article 32."

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.

RySG Response: Section 3.9 repeats a high level GDPR principle for data processing contained in Articles 32-36. The inclusion is therefore in anticipated compliance with the requirements of Article 28(3)(f), whereby a processor is required, per the required written agreement, to "assist[] the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36."

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.

RySG Response: Section 3.10 repeats a high level GDPR principle for data processing contained in Articles 44 and 45 (i.e. Chapter V). The inclusion is therefore in anticipated compliance with the requirements of Article 28(3)(a), whereby a processor is required to "processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation".

3.11. **Cooperating with Supervisory Authorities.** Cooperating with Supervisory Authorities, on request, in the performance of their tasks.

RySG Response: Section 3.11 repeats a high level GDPR principle for data processing contained in Article 31. The inclusion is therefore in anticipated compliance with the requirements of Article 28(1), whereby a processor is required to "meet the requirements of [the GDPR]."