~~Appendix C:~~ Data Processing Principles ~~Requirements~~

This Appendix sets out the ~~framework~~ principles 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~~ sets out 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.

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 and other applicable data protection law, 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~~i.e., make a commitment to provide a standard notice (to be developed by ICANN) that is concise, transparent, plain language, etc. for RDDS/WHOIS.

~~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. ICANN should identify specific operational requirements appropriate for the RDDS/WHOIS data, and include them in the applicable contract. ~~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 and applicable data protection law. 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.~~

3.x **Standard terms applicable to the Third parties.** Standard access agreement terms should be specified in the RAA to apply to the Third parties who seek to access the data in accordance with legitimate purposes with legal bases as specified in GDPR Art. 6.