RRA Data Processing Addendum

This RRA DATA PROCESSING ADDENDUM (the "**Data Processing Addendum**") is made by and between Public Interest Registry (the "**Registry**") and the undersigned registrar (the "**Registrar**") (each a "**Party**" and together the "**Parties**"), and is effective as of May 25, 2018, and supplements the terms and conditions of the Registry-Registrar Agreements in effect and (each an "**RRA**") executed between the Parties.

To the extent of any conflict between the RRA, as amended (including any of its attachments), and this Data Processing Addendum, the terms of this Data Processing Addendum will take precedence. Capitalized terms not defined below will have the meaning provided to them in the RRA.

1. INTRODUCTION

This Data Processing Addendum establishes the Parties' respective responsibilities for the Processing of Shared Personal Data under the RRA. It is intended to ensure that Shared Personal Data is Processed in a manner that is secure and in accordance with Applicable Laws and its defined Purpose(s). Though this Data Processing Addendum is executed by and between the Registry and Registrar as an addendum to the RRA, Purposes for Processing are often at the direction or requirement of ICANN as a Controller. Certain Purposes for Processing under the RAA may also be at the direction of the Registrar or Registry, each as a Controller.

2. DEFINITIONS

a) <u>Applicable Agreements</u>. Collectively means this Data Processing Addendum, the Registrar Accreditation Agreement ("**RAA**"), the Registry Agreement ("**RA**"), and the RRA, as those documents are applicable and binding on any individual Party.

b) <u>Applicable Laws</u>. The General Data Protection Regulation (2016/679) ("**GDPR**"), the Electronic Communications Data Protection Directive (*2002/58/EC*), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2426/2003*) (as amended) and all other applicable laws and regulations worldwide, including their successors or as modified, relating to the Processing of Shared Personal Data.

c) <u>Disclosing Party</u>. Means the Party that transfers Shared Personal Data to the Receiving Party.

d) <u>Data Protection Authority</u>. Means the relevant and applicable supervisory data protection authority in the member state or other territory where a Party to this Data Processing Addendum is established or has identified as its lead supervisory authority, or otherwise has jurisdiction over a Party to this Data Protection Addendum.

e) <u>Data Security Breach</u>. A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Shared Personal Data, and which is further subject to the provisions of Section 6 below.

f) <u>Data Subject</u>. Means an identifiable natural person who can be identified, directly or indirectly, in particular by reference to Personal Data.

g) <u>Personal Data</u>. Means any information such as a name, an identification number, location data, an online identifier or information pertaining to an individual's physical, physiological, genetic, mental, economic, cultural or social identity relating to that natural person, that can be used to directly or indirectly identify a Data Subject.

h) <u>Processing</u>. Means any operation or set of operations which is performed on the Shared Personal

Data, whether or not by automated means, and which includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing, Processes, Processed or other derivatives as used herein, will have the same meaning.

i) <u>Purpose(s)</u>. Has the meaning provided in Section 3 below.

j) <u>Receiving Party</u>. Means the Party receiving Shared Personal Data from the Disclosing Party.

k) <u>Registration Data</u>. Means data collected by the Registrar under the RAA and that is required to be shared with the Registry under the RAA and the RA.

l) <u>Shared Personal Data</u>. Means Personal Data contained in the fields within Registration Data and that is Processed in accordance with the Applicable Agreements.

m) <u>Temporary Specification</u>. Means the "Temporary Specification for gTLD Registration Data" Adopted on 17 May 2018 by the ICANN Board of Directors, as may be amended or supplemented from time to time.

3. PURPOSE, SUBJECT MATTER, AND ROLES

a) <u>Purpose(s)</u>. Processing of Shared Personal Data under this Data Processing Addendum by the Parties is for the limited purpose of provisioning, servicing, managing and maintaining domain names, as required of Registries and Registrars under the Applicable Agreements with ICANN, including to the extent those purposes serve to ensure the stability and security of the Domain Name System and to support the lawful, proper and legitimate use of the services offered by the Parties. Only Shared Personal Data is subject to the terms of this Data Processing Addendum.

b) <u>Subject Matter</u>. This Data Processing Addendum sets out the framework for the protection of Shared Personal Data for the Purposes noted in this section 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 necessitated by the Purpose(s) is to be performed at different stages, or at times even simultaneously by the Parties. Thus, this Data Processing Addendum is required to ensure that where Shared Personal Data may be Processed, it is done so at all times in compliance with the requirements of Applicable Laws.

c) <u>Roles and Responsibilities</u>. The Parties acknowledge and agree that, with respect to Processing of Shared Personal Data for the Purposes of this Data Processing Addendum:

   i. The details of Processing are established and set forth in <u>Annex 1</u>;

   ii. Each Party and ICANN may act as either a Controller or Processor of Shared Personal Data as specified in Appendix C to the Temporary Specification; and

   iii. Although ICANN, the Registry and Registrar may each take on the role, or additional role, of Controller or Processor in the lifecycle of processing Registration Data under Applicable Agreements, for the purposes of this Data Processing Addendum, only the roles of the Registry and the Registrar are applicable.

   iv. To the extent either the Purpose(s) or Subject Matter is not specifically referenced or noted when detailing the respective or shared rights, duties, liabilities or obligations hereunder, the Parties nonetheless mutually acknowledge and agree that the Purpose(s) and Subject Matter is and will be at all times the basis upon which legitimate and lawful processing hereunder may be conducted and performed.

4. FAIR AND LAWFUL PROCESSING

a)   Each Party shall ensure that it processes the Shared Personal Data fairly and lawfully in accordance with this Data Processing Addendum and Applicable Laws.

b)   Each Party shall ensure that it processes Shared Personal Data on the basis of one of the following legal grounds:

i.   The Data Subject has given consent to the Processing of his or her Personal Data for one or more specific Purposes;

ii.   Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;

iii.   Processing is necessary for compliance with a legal obligation to which the Controller is subject;

iv.   Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data; or

v.   Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller.

5. PROCESSING SHARED PERSONAL DATA

a)   All Parties agree that they are responsible for Processing of Shared Personal Data in accordance with Applicable Laws and this Data Processing Addendum. The Parties shall fully cooperate with each other to the extent necessary to effectuate corrections, amendments, restrictions or deletions of Personal Data as required by Applicable Laws and/or at the request of any Data Subject.

b)   A Party may only transfer Shared Personal Data relating to EU individuals to outside of the European Economic Area ("**EEA**") (or if such Shared Personal Data is already outside of the EEA, to any third party also outside the EEA), in compliance with the terms of this Data Processing Addendum and the requirements of Applicable Laws, the latter including any relevant Adequacy Decision of the European Commission or the use of EU 'Standard Contractual Clauses'. Where Standard Contractual Clauses for data transfers between EU and non-EU countries are required to be executed between the Parties, they may be found and downloaded, to be incorporated herein as part of this Data Processing Addendum upon execution, at   https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087 (or such link location as may be updated from time to time).

Those Standard Contractual Clauses are attached hereto and incorporated herein as Annex 2: Standard Contractual Clauses. For purposes of the RRA, the Registrar assumes and agrees to the obligations of the "Data Importer" as defined and set forth in the Standard Contractual Clauses and the Registry assumes and agrees to the obligations of the defined "Data Exporter" in the Standard Contractual Clauses. The Parties explicitly agree to be bound by the terms of the Standard Contractual Clauses as if they had separately signed them in each instance for the respective Data Importer and Data Exporter.

c)   A Party must immediately notify the other Party and ICANN if, in its opinion, ICANN's instructions or requirements under Applicable Agreements infringes any Applicable Laws.

d) All Shared Personal Data must be treated as strictly confidential and a Party must inform all its employees or approved agents engaged in processing the Shared Personal Data of the confidential nature of the Shared Personal Data, and ensure that all such persons or parties have signed an appropriate confidentiality agreement to maintain the confidence of the Shared Personal Data.

e) Where a Party Processes Shared Personal Data, it acknowledges and agrees that it is responsible for maintaining appropriate organizational and security measures to protect such Shared Personal Data in accordance with all Applicable Laws. Appropriate organizational and security measures are further enumerated in Section 5 of this Data Processing Addendum, but generally must include:

   i. Measures to ensure that only authorized individuals for the Purposes of this Data Processing Addendum can access the Shared Personal Data;

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

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

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

   v. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Shared Personal Data; and

   vi. Measures to identify vulnerabilities with regard to the processing of Shared Personal Data in its systems.

f) To the extent that the Receiving Party contracts with any subcontractor, vendor or other third-party to facilitate its performance under the Applicable Agreements, it must enter into a written agreement with such third party to ensure such party also complies with the terms of this Data Processing Addendum.

g) The Party which employs a sub-processor, vendor or other third-party to facilitate its performance under this Data Processing Addendum is and will remain fully liable for any such third party's acts where such party fails to fulfill its obligations under this Data Processing Addendum (or similar contractual arrangement put in place to impose equivalent obligations on the third party to those incumbent on the Receiving Party under this Data Processing Addendum) or under Applicable Laws.

h) Each Party will, at its expense, defend, indemnify and hold the other Party harmless from and against all claims, liabilities, costs and expenses arising from or relating to (i) a Data Security Breach, (ii) breach of Applicable Laws, and (iii) breach of this Data Processing Addendum, to the extent the cause of the breaching Party's negligent, willful or intentional acts or omissions.

i) The Parties shall, in respect of Shared Personal Data, 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 is included in Shared Personal Data, the circumstances in which it will be shared, the purposes for the Personal Data sharing and either the identity with whom the Personal Data is shared or a description of the type of organization that will receive the Shared Personal Data.

j) The Parties undertake to inform Data Subjects of the Purposes for which it will process the Shared 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.

k) The Shared Personal Data must not be irrelevant or excessive with regard to the Purposes.

l) A Party shall, subject to the instructions of the Data Subject, ensure that Shared Personal Data is accurate. Where any Party becomes aware of inaccuracies in Shared Personal Data, they will, where necessary, notify the other Parties, to enable the timely rectification of such data.

6. SECURITY

a) The Disclosing Party shall be responsible for the security of transmission of any Shared Personal Data in transmission to the Receiving Party by employing appropriate safeguards and technical information security controls.

b) All Parties agree to implement appropriate technical and organizational measures to protect the Shared Personal Data in their possession against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, including but not limited to:

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

   ii. Not leaving portable equipment containing the Shared Personal Data unattended;

   iii. Ensuring use of appropriate secure passwords for logging into systems or databases containing Shared Personal Data;

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

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

   vi. 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 Shared Personal Data, and ensuring that password security mechanisms are in place to prevent inappropriate access when individuals are no longer engaged by the Party;

   vii. Conducting regular threat assessment or penetration testing on systems as deemed necessary, considering the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, with due regard to the nature of the data held, the cost of implementation, and the state of the art;

   viii. Ensuring all authorized individuals handling Shared Personal Data have been made aware of their responsibilities with regards to handling of Shared Personal Data; and

   ix. Allowing for inspections and assessments to be undertaken by the Controller as to the security measures taken, or producing evidence of those measures, if requested.

7. SECURITY BREACH NOTIFICATION

a) <u>Notification Timing</u>. Should a Party become aware of any Data Security Breach by a sub-processor in relation to Shared Personal Data, and where such a Breach is of a material impact

to this Data Processing Addendum, or is likely to have a material impact on the Parties, the relevant Party should immediately notify the Parties, and the relevant Party shall provide immediate feedback about any impact this incident may/will have on the affected Parties, including the anticipated impacts to the rights and freedoms of Data Subjects if applicable. Such notification will be provided as promptly as possible, but in any event no later than 24 hours after detection of the Data Security Breach. Nothing in this section should be construed as limiting or changing any notification obligation of a Party under Applicable Laws.

b) <u>Notification Format and Content</u>. Notification of a Data Security Breach will be in writing to the information/administrative contact identified by the Parties, though communication may take place first via telephone. The notifying Party must be provided the following information, to the greatest extent possible, with further updates as additional information comes to light:

   i. A description of the nature of the incident and likely consequences of the incident;

   ii. Expected resolution time (if known);

   iii. A description of the measures taken or proposed to address the incident including, measures to mitigate its possible adverse effects the Parties and/or Shared Personal Data;

   iv. The categories and approximate volume of Shared Personal Data and individuals potentially affected by the incident, and the likely consequences of the incident on that Shared Personal Data and associated individuals; and

   v. The name and phone number of a representative the Party may contact to obtain incident updates.

c) <u>Security Resources.</u> The Parties' may, upon mutual agreement, provide resources from its security group to assist with an identified Data Security Breach for the purpose of meeting its obligations in relation to the notification of a Data Security Breach under Applicable Laws or other notification obligations or requirements.

d) <u>Failed Security Incidents</u>. A failed security incident will not be subject to the terms of this Data Processing Addendum. A failed security incident is one that results in no unauthorized access or acquisition to Shared Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

e) <u>Additional Notification Requirements</u>. For the purpose of this section, a Party is also required to provide notification in accordance with this section in response to:

   i. A complaint or objection to Processing or request with respect to the exercise of a Data Subject's rights under Applicable Laws; and

   ii. An investigation into or seizure of Shared Personal Data by government officials, regulatory or law enforcement agency, or indications that such investigation or seizure is contemplated.

8. DATA SUBJECT RIGHTS

a) Controllers have certain obligations to respond to requests of a Data Subject whose Personal Data is being processed under this Data Processing Addendum, and who wishes to exercise any of their rights under Applicable Laws, including, but not limited to: (i) right of access and

update; (ii) right to data portability; (iii) right to erasure; (iv) right to rectification; (v) right to object to automated decision-making; or (vi) right to object to processing.

b) Data Subjects have the right to obtain certain information about the processing of their personal data through a subject access request ("**Subject Access Request**"). The Parties shall maintain a record of Subject Access Requests, the decisions made and any information that was exchanged. Records must include copies of the request for information, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request.

c) The Parties agree that the responsibility for complying with a Subject Access Request falls to the Party receiving the Subject Access Request in respect of the Personal Data held by that Party, but any final decisions made by the Controller will govern.

d) The Parties agree to provide reasonable and prompt assistance (within 5 business days of such a request for assistance) as is necessary to each other to enable them to comply with Subject Access Requests and to respond to any other queries or complaints from Data Subjects.

9. DATA RETENTION AND DELETION

Notwithstanding any requirements under the Applicable Agreements to the contrary, the Parties will retain Shared Personal Data only as necessary to carry out the Purposes or otherwise in accordance with the Temporary Specification and as permitted under Applicable Laws, and thereafter must delete or return all Shared Personal Data accordingly.

10. TRANSFERS

a) For the purposes of this Data Processing Addendum, transfers of Personal Data include any sharing of Shared Personal Data, and shall include, but is not limited to, the following:

   i. Transfers amongst the Parties for the Purposes contemplated in this Data Processing Addendum or under any of the Applicable Agreements;

   ii. Disclosure of the Shared Personal Data with any other third party with a valid legal basis for the provisioning of the Purposes;

   iii. Publication of the Shared Personal Data via any medium, including, but not limited to in public registration data directory services;

   iv. The transfer and storage by the Receiving Party of any Shared Personal Data from within the EEA to servers outside the EEA; and

   v. Otherwise granting any third party located outside the EEA access rights to the Shared Personal Data.

b) No Party shall disclose or transfer Shared Personal Data outside the EEA without ensuring that adequate and equivalent protections will be afforded to the Shared Personal Data.

11. RESOLUTION OF DISPUTES

a) In the event of a dispute or claim brought by a Data Subject or an applicable Data Protection Authority against any Party concerning the processing of Shared Personal Data, the concerned Parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b) The Parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by a Data Protection Authority. If they do participate in the

proceedings, the Parties may elect to do so remotely (such as by telephone or other electronic means). The Parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c) In respect of Data Security Breaches or any breach of this Data Processing Addendum, each Party shall abide by a decision of a competent court of the complaining Party's country of establishment or of any binding decision of the relevant Data Protection Authority.

12. IMPACT OF CHANGES; NEW GUIDANCE

In the event the ICANN Board adopts changes to the Temporary Specification (a "**Triggering Event**"), then Registry may notify Registrar of the changes, and upon ICANN publication of the updated Temporary Specification to its website, the changes will also be adopted and incorporated automatically herein to this Data Processing Addendum.

Registrar will be given thirty (30) days to accept or reject the proposed changes; rejection may result in termination of the RRA. If Registrar does not respond within thirty (30) days following notice, it is deemed to have accepted the changes to the Data Processing Addendum, as applicable.

In the event Applicable Laws change in a way that the Data Processing Addendum is no longer adequate for the purpose of governing lawful processing of Shared Personal Data and there was no Triggering Event, the Parties agree that they will negotiate in good faith to review and update this Data Processing Addendum in light of the new laws.

PUBLIC INTEREST REGISTRY   [Registrar] _____

By: _____   By: _____

Name:_____   Name:_____

Title: _____   Title: _____

DETAILS OF THE PROCESSING

1. **Nature and Purpose of Processing**. The Parties will Process Shared Personal Data only as necessary to perform under and pursuant to the Applicable Agreements, and subject to this Data Processing Addendum, including as further instructed by Data Subjects.

2. **Duration of Processing**. The Parties will Process Shared Personal Data during the Term of the underlying RRA to which this this Data Processing Addendum is applicable, but will abide by the terms of this Data Processing Addendum for the duration of the Processing if in excess of that term, and unless otherwise agreed upon in writing.

3. **Type of Personal Data**. Data Subjects may provide the following Shared Personal Data in connection with the purchase of a domain name from a Registrar:

Registrant Name: Example Registrant
Street: 1234 Admiralty Way
City: Marina del Rey
State/Province: CA
Postal Code: 90292
Country: US
Phone Number: +1.3105551212
Fax Number: +1.3105551213
Email: registrant@example.tld
Admin Contact: Jane Registrant
Phone Number: +1.3105551214
Fax Number: +1.3105551213
Email: janeregistrar@example-registrant.tld
Technical Contact: John Geek
Phone Number: +1.3105551215
Fax Number: +1.3105551216
Email: johngeek@example-registrant.tld

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

_____

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: Public Interest Registry..

Address: 1775 Wiehle Avenue, Suite 100, Reston, VA, 20190, USA......................................

Tel.:+1 (703) 889-5778 ....; fax: +1 (703) 889-5779..; e-mail:privacy@pir.org ....

Other information needed to identify the organisation:

……………………………………………………………
(the data **exporter**)

And

Name of the data importing organisation:The "Registrar" as defined in the RRA Data Processing Addendum

Address: ....

Tel.: ....; fax: ....; e-mail: ....

Other information needed to identify the organisation:

……………………………………………………………
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the Personal Data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a)   *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data[1];

(b)   '*the data exporter'* means the controller who transfers the personal data;

(c)   *'the data importer'* means the processor who agrees to receive from the data exporter Personal Data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d)   *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer Personal Data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e)   '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of Personal Data applicable to a data controller in the Member State in which the data exporter is established;

(f)   *'technical and organisational security measures'* means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of Personal Data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

---

[1]   Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the Personal Data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the Personal Data processing services will instruct the data importer to process the Personal Data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate

to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e)   that it will ensure compliance with the security measures;

(f)   that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g)   to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h)   to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i)   that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the Personal Data and the rights of data subject as the data importer under the Clauses; and

(j)   that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a)   to process the Personal Data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b)   that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

---

[2]   Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(c)   that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the Personal Data transferred;

(d)   that it will promptly notify the data exporter about:

   (i)   any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

   (ii)   any accidental or unauthorised access, and

   (iii)   any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e)   to deal promptly and properly with all inquiries from the data exporter relating to its processing of the Personal Data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f)   at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g)   to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h)   that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i)   that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j)   to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1.   The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2.   If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data

exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3.   If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1.   The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a)   to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b)   to refer the dispute to the courts in the Member State in which the data exporter is established.

2.   The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1.   The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2.   The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3.   The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely the Republic of Ireland (through its representative).

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1.   The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2.   The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.   The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely the Republic of Ireland (through its representative).

4.   The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

---

[3]   This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Obligation after the termination of Personal Data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the Personal Data transferred and the copies thereof to the data exporter or shall destroy all the Personal Data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the Personal Data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:
Name (written out in full): Public Interest Registry
Position: The signatory to the RRA Data Processing Addendum
Address: 1775 Wiehle Avenue, Suite 100, Reston, VA, 20190, USA
Other information necessary in order for the contract to be binding (if any):

Signature: Agreed to by the Registry in the RRA Data Processing Addendum

(stamp of organisation)

On behalf of the data importer:
Name (written out in full): The "Registrar" as defined in the RRA Data Processing Addendum
Position: The signatory to the RRA Data Processing Addendum
Address: The "Registrar" as defined in the RRA Data Processing Addendum
Other information necessary in order for the contract to be binding (if any):

Signature: Agreed to by the Registrar in the RRA Data Processing Addendum

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer): as the registry operator for several top-level domains(.org, .ong, .ngo, .opr (xn--c1avg), .机构 (xn--nqv7f), .संगठन (xn--i1b6b1a6a2e), .组织机构(xn--nqv7fs00ema)), PIR operates (via a technical backend provider) registries to provide domain name registration services to registrants through registrars in line with PIR's contractual requirements with the Internet Corporation for Assigned Names and Numbers (ICANN).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):
The Registrar processes registrant data for the fulfillment and maintence of domain name registrations in line with PIR's contractual requirements with ICANN. This can include the processing the data of both natural and legal persons and potential third-country transfers.

Data subjects

The Personal Data transferred concern the following categories of data subjects (please specify): Natural person's data can include registrant's information provided to registrars upon registration of a domain name noted in Annex 1 (3) of the RRA Data Processing Addendum (registrant name, address, email, phone number, IP address) commonly known as "WHOIS" data. The Registrar processes the same information for legal persons or entities.

Categories of data

The Personal Data transferred concern the following categories of data (please specify): Natural person's data can include registrant's information provided to registrars upon registration of a domain name (registrant name, address, email, phone number, IP address) commonly known as "WHOIS" data.

Special categories of data (if appropriate)

The Personal Data transferred concern the following special categories of data (please specify): N/A

Processing operations

The Personal Data transferred will be subject to the following basic processing activities (please specify):Receipt of above outlined data by PIR (and/or the technical backend provider) from the Registrar. Following transfer, the Registry (and/or the technical backend provider) and the Registar will store, delete, alterater for accuracy, disclosure (only on legitimate bases), maintenance, and analysis.

DATA EXPORTER
Name: Public Interest Registry
Authorised Signature: Agreed to by the Registry in the RRA Data Processing Addendum
DATA IMPORTER
Name: The "Registrar" as defined in the RRA Data Processing Addendum
Authorised Signature: Agreed to by the Registrar in the RRA Data Processing Addendum