DATA PROCESSING SPECIFICATION

The Internet Corporation for Assigned Names and Numbers ("ICANN") and [INSERT REGISTRY OPERATOR NAME] agree, effective as of [•], 202[•], that this Data Processing Specification shall be annexed to and incorporated in the [Registry Agreement], dated as of [INSERT EFFECTIVE DATE] (the "Agreement"), for the top-level domain "[.TLD]" (the "TLD"). All capitalized terms not defined in this Data Processing Specification shall have the meaning given to them elsewhere in the Agreement. The Agreement does not define the requirements and responsibilities of the parties when Processing Personal Data for purposes other than those specified in the Agreement. Processing Personal Data outside of the scope of the Agreement is the sole responsibility of the respective party.

1. DEFINITIONS

The following terms shall have the following meanings for purposes of this Data Processing Specification, provided that such terms or any derivation thereof shall not define any term used elsewhere in the Agreement.

1.1. "Applicable Data Protection Laws" means a law or regulation applicable to a party that governs the Processing of Personal Registration Data under the Agreement, including the security and localization of such data, including, but not limited to, the European Union's ("EU") General Data Protection Regulation (2016/679) ("GDPR") and its respective implementing laws.

1.2. "Data Protection Authority" means any competent supervisory data protection authority in the jurisdiction of a party or that otherwise has jurisdiction over a party to this Agreement (e.g., a lead supervisory authority).

1.3. "Data Security Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Registration Data.

1.4. "Data Subject" means an identified or identifiable natural person who is the subject of Personal Data.

1.5. "Personal Data" means any information that can be used to directly or indirectly identify a Data Subject, 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.

1.6. "Personal Registration Data" means the Personal Data collected pursuant to the Registration Data Policy, this Agreement, or any registrar accreditation agreement from a natural or legal person in connection with a registered name.

1.7. "Processing" means any operation or set of operations performed on Personal Registration Data, whether or not by automated means, such as 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. "Process," "Processes," "Processed," or other derivatives of Processing capitalized and used herein will have the same meaning.

1.8. "Purpose" means the purposes for the parties' Processing of Personal Registration Data as described in Section 2 of this Data Processing Specification.

1.9. "Registration Data Policy" means the Registration Data Policy effective as of [•], available at [•].

1.10. "Service Provider" means any subcontractor, vendor, or other third party carrying out Processing activities pursuant to this Data Processing Specification, registry agreements, registrar accreditation agreements, or the Registration Data Policy on behalf of a party.

2. PURPOSES FOR PROCESSING

2.1. The parties Process Personal Registration Data under the Agreement for the following limited Purposes:

2.1.1. In accordance with the relevant registry agreements and registrar accreditation agreements, to activate a registered name and allocate it to the registered name holder;

2.1.2. Subject to the registry and registrar terms, conditions, policies, and ICANN Consensus Policies, to:

2.1.2.1. Establish the rights of a registered name holder in a registered name, and

2.1.2.2. Ensure that a registered name holder may exercise its rights in the use, maintenance, and disposition of the registered name;

2.1.3. Contribute to the maintenance of the security, stability, and resiliency of the domain name system in accordance with ICANN's mission;

2.1.4. Enable communication with the registered name holder on matters relating to the registered name;

2.1.5. Provide mechanisms for safeguarding registered name holders' registration data in the event of a business or technical failure of a registrar or Registry Operator, or unavailability of a registrar or Registry

Operator, as described in registrar accreditation agreements and the Agreement respectively;

2.1.6. Handle contractual compliance monitoring requests and audit activities consistent with the terms of the Agreement and the registrar accreditation agreements and any applicable processing agreements, by Processing specific data only as necessary;

2.1.7. Handle compliance complaints initiated by ICANN or third parties consistent with the terms of the Agreement and the registrar accreditation agreements;

2.1.8. Operationalize policies for the resolution of disputes regarding or relating to the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names), namely, the Uniform Domain Name Dispute Resolution Policy ("UDRP"), the Uniform Rapid Suspension System ("URS"), the Trademark Post-Delegation Dispute Resolution Procedure ("PDDRP"), the Registration Restrictions Dispute Resolution Procedure ("RRDRP"), and the Registrar Transfer Dispute Resolution Policy ("TDRP"); and

2.1.9. Enable validation to confirm that registered name holders meet the eligibility criteria voluntarily adopted by a Registry Operator and that are described or referenced in the Registry Agreement for that generic top-level domain ("gTLD").

3. RESPONSIBILITIES

3.1. Each party acknowledges that the role (as a controller, processor, or similar concepts or terms under Applicable Data Protection Laws) and the related responsibilities of a party for the Processing of the Personal Registration Data are attributed on the basis of an assessment of all relevant factual circumstances.

3.2. The assessment of all relevant factual circumstances (referred to in the foregoing Section 3.1 of this Data Processing Specification) includes an assessment of the contractual relations between ICANN, registry operators, and registrars, as laid out in the applicable registrar accreditation agreements, applicable registry agreements, Registration Data Policy, and the actual Processing activities carried out by ICANN, registry operators, and registrars in this regard, as further set forth in Annex 1 to this Data Processing Specification.

4. PROCESSING OF REGISTRATION DATA

4.1. Each party shall Process Personal Registration Data in accordance with (i) the Agreement (excluding this Data Processing Specification), (ii) this Data Processing

Specification, (iii) the Registration Data Policy, and (iv) Applicable Data Protection Laws.

4.2. When either party transfers Personal Registration Data in a manner subject to cross-border data transfer restrictions under Applicable Data Protection Laws, for example a transfer of Personal Registration Data from the European Economic Area ("EEA") to a non-EEA party or third party, the transferring party shall ensure that such transfers take place in compliance with Applicable Data Protection Laws, including, if applicable, the implementation of necessary transfer safeguards under such laws (e.g., EU Standard Contractual Clauses ("SCCs"), obtaining consent from Data Subjects and authority approval). The SCCs for transfers between controllers (Commission Implementing Decision (EU) 2021/914 of 4 June 2021) ("SCCs C-t-C") in Annex 2, including their Appendix and the Annexes, apply to transfers of Personal Registration Data as further specified in Annex III, which contains operative provisions for the implementation of the SCCs C-t-C, subject to cross-border data transfer restrictions under Applicable Data Protection Laws of the EEA, the United Kingdom ("UK") and Switzerland, from registry operators to ICANN establishments in third countries and shall be incorporated herein as part of this Data Processing Specification. If the SCCs C-t-C are repealed or amended by a Commission Decision, the new or amended version of the SCCs C-t-C shall automatically replace the SCCs C-t-C in Annex 2 and shall be deemed effective two (2) months after the Commission Decision on the new or amended version of the SCCs C-t-C entered into force. The parties must have agreed within this two-month (2) period on a language version of the new or amended version of the SCCs C-t-C, which shall be posted publicly on ICANN's website prior to the end of the two-month (2) period. The foregoing mechanism shall apply accordingly if the SCCs C-t-C have to be amended or supplemented, or if changes to the description of the transfers of Personal Registration Data in Annex I.B. to the SCCs are required, due to a change of the underlying factual circumstances or pursuant to requirements of Applicable Data Protection Laws or mandatorily applicable guidance of authorities.

4.3. Each party shall ensure that all its employees, Services Providers, or any other persons acting on its behalf, who are authorized to Process Personal Registration Data and have access thereto, have acknowledged confidentiality and Processing obligations that meet the requirements of Applicable Data Protection Laws.

4.4. The parties shall: (i) provide privacy notices if required by, and in accordance with, Applicable Data Protection Laws, and (ii) reasonably assist each other with meeting their respective information (notice) obligations under Applicable Data Protection Laws, including, for the parties to provide Data Subjects with a reference (such as a link) to the Registry Operator's or ICANN's relevant privacy notice or policy.

4.5. If a party contracts with any Service Provider, the party shall enter into a written agreement with such third party as required under Applicable Data Protection

Laws, including data processing agreements pursuant to Art. 28 of the GDPR, if applicable.

4.6. Each party will make publicly available, where applicable, the contact details for their EEA Representative in accordance with Article 27 of the GDPR or data protection officer where required by Applicable Data Protection Laws.

5. SECURITY OF PERSONAL REGISTRATION DATA

5.1. Each party has implemented and will maintain appropriate technical and organizational measures for Processing Personal Registration Data in accordance with (i) the Agreement (excluding this Data Processing Specification), (ii) this Data Processing Specification, (iii) the Registration Data Policy, and (iv) Applicable Data Protection Laws in order to ensure the security of the Personal Registration Data.

5.2. In assessing the appropriate level of security, the parties shall take due account of the risks involved in the Processing, the nature of the Personal Registration Data, and the nature, scope, context, and purposes of Processing.

5.3. Each party must develop a security policy that describes the technical and organizational measures implemented and maintained pursuant to Sections 5.1 and 5.2. In general, the security policy should include provisions on:

5.3.1. An inventory of all hardware and software utilized by registration data systems to Process Personal Registration Data;

5.3.2. The update policy of all hardware and software utilized by registration data systems to Process Personal Registration Data;

5.3.3. The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of registration data systems and of all hardware and software utilized by such systems, including encryption measures and their implementation and maintenance;

5.3.4. The measures to limit access to only such individuals who are authorized to Process Personal Registration Data; and

5.3.5. The processes for regular testing, assessing, and evaluating the effectiveness of the technical and organization measures described in the security policy.

6. SECURITY BREACH NOTIFICATION

6.1. Notification Timing. If ICANN becomes aware of any Data Security Breach relating to its Processing of Personal Registration Data, which concerns the Personal Registration Data of a registered name holder in a TLD of Registry

Operator, it shall notify Registry Operator as soon as practicable. If Registry Operator becomes aware of any Data Security Breach relating to its Processing of Personal Registration Data, Registry Operator shall notify ICANN as required by Applicable Data Protection Laws.

6.2. Notification Format and Content. Notification of a Data Security Breach must be in writing via email or other secure method of electronic communication authorized by ICANN to an information or administrative contact identified by the parties (which shall be identified by the parties promptly following the date of this Data Processing Specification and updated as necessary to replace such contact), though communication may take place first via telephone. Any other provisions specifying the manner in which notice is to be provided under the Agreement or the content of such notice do not apply to the notification of a Data Security Breach pursuant to this Section 6 of the Data Processing Specification. Concurrent with the notification provided pursuant to Section 6.1, the notifying party must, to the greatest extent possible, provide the information described in Sections 6.2.1 through Section 6.2.5 below, and shall thereafter regularly update, as additional information becomes available, the information provided to the other party pursuant to this Section 6.2.

6.2.1. A reasonably detailed description of the nature of the incident;

6.2.2. Expected resolution time (if known);

6.2.3. A description of the measures taken or proposed to address the incident, including measures to mitigate the incident's possible adverse effects on Data Subjects and the parties;

6.2.4. The categories and approximate volume of Personal Registration Data and Data Subjects potentially affected by the incident, and an assessment of the likely risks to and consequences of the incident on that Personal Registration Data and associated Data Subjects; and

6.2.5. The name, email address, and telephone number of a representative of the notifying party with up-to-date knowledge of the incident who may be contacted to obtain incident updates.

6.3. Security Resources. The parties may, upon mutual agreement, cooperate to assist the other party with an identified Data Security Breach for the purpose of meeting such other party's obligations in relation to the notification of a Data Security Breach under Applicable Data Protection Laws.

6.4. External Communication. Registry Operator and ICANN agree to not publicly disclose any information concerning a Data Security Breach without first notifying the other party with regards to the content of such disclosure and providing a reasonable amount of time for the other party to provide comments, provided that

ICANN shall only be obligated to notify the Registry Operator of any such intended external communication if, to ICANN's knowledge, such Data Security Breach (to which the communication relates) concerned Personal Registration Data of a registered name holder in a TLD of the Registry Operator. Any disclosure required under applicable laws (including any disclosure concerning a Data Security Breach required by Applicable Data Protection Laws) or contemplated under the ICANN Bylaws is not subject to the requirements of this Section 6.4.

7. DATA SUBJECT RIGHTS

7.1. Each party shall handle requests from Data Subjects relating to the Processing of Personal Registration Data in a manner consistent with Applicable Data Protection Laws, including but not limited to, Data Subjects' exercise of rights related to (i) access, (ii) rectification, (iii) erasure, (iv) restriction of Processing, (v) data portability, (vi) objection to Processing, and (vii) automated decision-making.

7.2. Each party shall cooperate with the other, insofar as this is possible, and to the extent necessary to effectuate appropriate responses to Data Subjects' requests for exercising any of their rights under Applicable Data Protection Laws.

7.3. If ICANN's designated contact for Data Subject Access Requests receives a request from a Data Subject that provided Personal Registration Data to a registrar or whose Personal Registration Data were provided to a registrar, and that Data Subject is exercising its rights under Applicable Data Protection Laws with respect to the Personal Registration Data provided, ICANN must, without undue delay and in no event later than five (5) business days following receipt of such request, provide the Data Subject with information that will enable the Data Subject to identify and contact the relevant registrar (e.g., by making the Data Subject aware of the possibility of using the Domain Name Registration Data Lookup in order to identify the registrar). This obligation applies irrespective of an obligation of ICANN, if any, to respond to the request raised by the Data Subject.

7.4. Each party shall maintain a record of requests received from Data Subjects relating to the Processing of Personal Registration Data, the decisions made by such party in response to such requests, and any information that was provided by the Data Subject to such party for a minimum period of one (1) year after receiving the request, unless a different retention period is required or permitted under Applicable Data Protection Laws.

8. DATA RETENTION AND DELETION

The parties will retain Personal Registration Data only (i) as necessary to carry out the Purposes or otherwise in accordance with ICANN Consensus Policies or Temporary Policies and the Agreement, and (ii) as permitted under Applicable Data Protection Laws. If, at any time, any of the foregoing clauses (i) or (ii) is not satisfied, such party must

promptly delete or return all Personal Registration Data, unless further Processing is permitted under Applicable Data Protection Laws.

9. PROCESSING OF COMMUNICATIONS

9.1. If a party receives any complaint, notice, or communication from a Data Protection Authority or Data Subject which relates, directly or indirectly, to the other party's: (i) Processing of the Personal Registration Data; or (ii) potential failure to comply with Applicable Data Protection Laws as they relate to the Processing of Personal Registration Data, the receiving party shall, to the extent permitted by applicable law, as promptly as practicable, forward the complaint, notice, or communication to the other party (to an information or administrative contact identified by the party in accordance with Section 6.2; the notice provisions of the Agreement (in particular Section 7.9) shall not be applicable), provided that any non-willful failure to timely take such action shall not be a breach or failure to comply with this Section 9.1. Each party will provide the other party, upon the other party's request, with information reasonably required for the other party to respond to any such complaint, notice, or communication.

9.2. For the avoidance of doubt, the provisions of Section 9.1 of this Data Processing Specification shall not govern: (i) disputes or claims that are subject to UDRP, URS, PICDRP, RRDRP, or other third-party dispute resolution procedures available under the Agreement, or (ii) disputes or claims between Registry Operator and ICANN.

10. LIABILITY

10.1. To the extent permitted under Applicable Data Protection Laws, and except as provided in Section 10.3 below, each party's liability arising out of or related to this Data Processing Specification, including Clause 12 (a) of the SCCs C-t-C, but excluding Clauses 12 (b), (c) and (d) of the SCCs C-t-C, whether in contract, tort or under any other theory of liability, is subject to the limitations of liability set forth in Section 5.3 of the Agreement.

10.2. Except as provided in Section 10.3 below, and solely with respect to third party claims arising from or in connection with Registry Operator's actual or alleged breach of this Data Processing Specification, Registry Operator's aggregate monetary indemnification obligations under Section 7.1 of the Agreement will be limited to the greater of (i) the fees paid to ICANN during the preceding twelve-month period (excluding the Variable Registry-Level Fee set forth in Section 6.3 of the Agreement, if any), or (ii) the amount of $5 million USD.

10.3. Notwithstanding anything to the contrary elsewhere in this Data Processing Specification or the Agreement, any limitation on indemnification obligations under this Section 10 will not apply to any claims (i) arising from or related to any act or omission involving the gross negligence, willful misconduct, or fraud on the

part of the Registry Operator, or (ii) directly arising from a failure of the Registry Operator to comply with laws applicable to the Registry Operator.

10.4. Nothing in this section will affect the remaining terms of the Agreement relating to liability, including any specific exclusions from any limitation of liability.

11. INCORPORATION BY REFERENCE; PRIORITY; COSTS

11.1. This Data Processing Specification is hereby incorporated in, and forms a part of, Article 2 of the Agreement, as if this Specification was set forth therein in its entirety.

11.2. Unless expressly stated otherwise in this Data Processing Specification, if any provisions of this Data Processing Specification conflicts with any other provisions of the Agreement (including any other Specification of the Agreement), such provision of the Data Processing Specification shall prevail and supersede the conflicting provisions of the Agreement. Any conflict between Section 4.1(iv) of this Data Processing Specification (Applicable Data Protection Laws) and any other provision of the Agreement (including any other Specification of the Agreement) is governed by Section 7.13 of the Agreement (Severability; Conflicts with Laws). Clause 5 of the SCCs C-t-C in Annex 2 shall remain unaffected.

11.3. Unless expressly stated otherwise in this Data Processing Specification, nothing in this Data Processing Specification waives any obligation on the parties under the Agreement, including obligations to comply with Consensus and Temporary Policies in existence today or that may be adopted in the future.

11.4. If Consensus Policy recommendations adopted by the ICANN Board of Directors have potential relevance to this Data Processing Specification, ICANN or the DPS Working Group may send a DPS Negotiation Notice and initiate a DPS Discussion Period. Any and all proposed amendments are subject to discretionary review and approval by ICANN and the DPS Working Group through the procedures described in Section 13 of this Data Processing Specification.

11.5. Each party shall bear its own respective costs incurred (i) in connection with the preparation of this Data Processing Specification and (ii) for the performance of its obligations under the Data Processing Specification, unless another allocation of costs has been expressly stipulated.

12. TERMINATION

12.1. Either ICANN or Registry Operator may terminate this Data Processing Specification for any or no reason upon sixty (60) calendar days advance notice to the other party. Any termination rights under the Agreement (excluding this Data Processing Specification) are applicable separately, provided, however, that either party may not exercise its termination rights under the Agreement (excluding the

Data Processing Specification) for breach of the Data Processing Specification, unless such breach is also a breach of the Agreement (excluding the Data Processing Specification). All other rights and remedies under the Agreement (excluding the Data Processing Specification) are unaffected and may be applied in the event of a breach of the Data Processing Specification. Nothing in this section will affect the parties' termination rights or other remedies under the Agreement (excluding the Data Processing Specification) for breaches of the Agreement (excluding the Data Processing Specification). In case the Data Processing Specification has been terminated pursuant to this Section 12.1, the terms of the Agreement (excluding this Data Processing Specification) will remain in full force and effect until the Agreement (excluding this Data Processing Specification) expires or is terminated in accordance with its terms. Except as set forth in this Section 12.1, this Data Processing Specification shall terminate automatically on termination or expiry of the Agreement, or as envisaged under the Approved DPS Amendment.

12.2. For the avoidance of doubt, the termination of this Data Processing Specification shall not relieve the parties of any obligation or breach accruing prior to such termination. This Section 12.2, Section 22, Section 4.1 (i), (iii) and (iv), Section 4.2, Section 10 and Section 14 as well as the contractual measures included in Annex 2 (e.g., SCCs C-t-C) shall survive the expiration or termination of this Data Processing Specification and shall continue to remain effective until they are (i) repealed by mutual agreement of the parties, or (ii) replaced by a new data protection agreement between the parties. The right to termination by either party contained in such contractual measures (e.g., Clause 16 of the SCCs C-t-C) shall remain unaffected.

13. AMENDMENT PROCEDURE

13.1. The terms of this Section define the process for amending this Data Processing Specification and supersede the amendment procedures in Section 7.7 of the Agreement. If the terms of this Section, at any time, conflict with any other provisions of the Agreement (including any other specification of the Agreement), the terms of this Section shall prevail and supersede the conflicting provisions of the Agreement. The provisions in Section 7.6 of the Agreement shall remain unaffected.

13.2. Definitions for the purposes of this Section.

13.2.1. "Applicable DPS Parties" means collectively, (i) the registry operators of top-level domains party to a registry agreement that contains this Data Processing Specification (or a materially similar data processing specification) and (ii) the registrars party to a registrar accreditation agreement that contains this Data Processing Specification (or a materially similar data processing specification), in each case to the

extent impacted by any proposed amendment subject to negotiation under this Section 13.2.1.

13.2.2. "DPS Chair" means the person appointed from the DPS Working Group by the chairperson of the Registry Stakeholder Group and the chairperson of the Registrar Stakeholder Group to serve as the chairperson of the DPS Working Group.

13.2.3. "DPS Working Group" means representatives of the Applicable DPS Parties and other members of the community that the Registry Stakeholder Group and the Registrar Stakeholder Group appoint, from time to time, to serve as a working group to consult on amendments to this Data Processing Specification (excluding bilateral amendments pursuant to Section 7.6(i) of the Agreement). For purposes of this Data Processing Specification, references to the Working Group in the Agreement means the DPS Working Group.

13.2.4. "DPS Working Group Approval" means approval by a consensus of the DPS Working Group following consultation with the relevant Stakeholder Group (Registry Stakeholder Group or Registrar Stakeholder Group as may be applicable).

13.3. If either the Chief Executive Officer of ICANN ("CEO") or the DPS Chair desire to discuss any revision(s) to this Data Processing Specification, the CEO or DPS Chair, as applicable, shall provide written notice to the other person, which shall set forth in reasonable detail the proposed revisions to this Data Processing Specification (a "DPS Negotiation Notice"); provided, however, that a DPS Negotiation Notice from the DPS Chair shall only be valid if accompanied by the written evidence of approval by [a consensus] of the DPS Working Group. Notwithstanding the foregoing, under this Section 13.3, neither the CEO nor the DPS Chair may (i) propose revisions to this Data Processing Specification that modify any Consensus Policy then existing or (ii) propose revisions to any other portion of the Agreement other than this Data Processing Specification.

13.4. Following receipt of the DPS Negotiation Notice by either the CEO or the DPS Chair, ICANN and the DPS Working Group shall consult in good faith negotiations regarding the substance of the proposed revisions to this Data Processing Specification, which shall be in the form of a proposed amended and restated version of this Data Processing Specification (the "DPS Proposed Revisions"), for a period of at least ninety (90) calendar days (unless a resolution is earlier reached) from receipt of the DPS Negotiation Notice and attempt to reach a mutually acceptable agreement relating to the DPS Proposed Revisions (the "DPS Discussion Period").

13.5. If an agreement is reached on the DPS Proposed Revisions, ICANN shall post the mutually agreed DPS Proposed Revisions on its website for public comment for no

less than thirty (30) calendar days (the "DPS Revisions Posting Period") and provide notice of such DPS Proposed Revisions to all Applicable DPS Parties in accordance with Section 13.6.4. ICANN and the DPS Working Group will consider the public comments submitted on the DPS Proposed Revisions during the DPS Revisions Posting Period (including comments submitted by the Applicable DPS Parties). Within sixty (60) calendar days of the conclusion of the DPS Revisions Posting Period, the DPS Proposed Revisions (with modifications, if any, to reflect and/or address input from ICANN, the DPS Working Group, and public comments (as applicable)) shall be submitted for DPS Working Group Approval and approval by the ICANN Board of Directors. If such approvals are obtained, the DPS Proposed Revisions shall be deemed approved (an "Approved DPS Amendment") by the Applicable DPS Parties and ICANN, and shall be effective and deemed an amendment and restatement to this Data Processing Specification upon sixty (60) calendar days' notice from ICANN to the Applicable DPS Party.

13.6. If, following the conclusion of the DPS Discussion Period, an agreement is not reached between ICANN and the DPS Working Group on the DPS Proposed Revisions, either the CEO or the DPS Chair may provide the other person written notice (the "DPS Mediation Notice") requiring ICANN and the DPS Working Group to attempt to resolve the disagreements related to the DPS Proposed Revisions through impartial, facilitative, non-evaluative, and non-binding mediation in accordance with the terms and conditions set forth below.

13.6.1. The mediation shall be conducted by a single mediator selected by the CEO and the DPS Chair. If the CEO and DPS Chair cannot agree on a mediator within fifteen (15) calendar days following delivery of the DPS Mediation Notice pursuant to Section 13.6, the CEO and DPS Chair will promptly select a mutually acceptable mediation provider entity, which shall, as soon as practicable following such entity's selection, designate a mediator who is a licensed attorney with expertise regarding the Applicable Data Protection Laws and general knowledge of contract law in the applicable jurisdiction(s) implicated by such DPS Proposed Revisions; who has no ongoing business relationship with either ICANN or any Applicable DPS Party; and, to the extent necessary to mediate the particular dispute, with general knowledge of the domain name system. Any mediator must confirm in writing that he or she is not, and will not become during the term of the mediation, an employee, partner, executive officer, director, or security holder of ICANN or an Applicable DPS Party. If such confirmation is not provided by the appointed mediator, then a replacement mediator shall be appointed pursuant to this Section 13.6.1.

13.6.2. The mediator shall conduct the mediation in accordance with the rules and procedures for facilitative mediation that he or she determines following consultation with the CEO and the DPS Chair.

Representatives of ICANN and the DPS Working Group shall discuss the dispute in good faith and attempt, with the mediator's assistance, to reach an amicable resolution of the dispute.

13.6.3. Each party shall bear its own cost in the mediation. The parties shall share equally the fees and expenses of the mediator.

13.6.4. If an agreement is reached during the mediation, ICANN shall post the mutually agreed DPS Proposed Revisions on its website for the DPS Revisions Posting Period and provide notice to all Applicable DPS Parties in accordance with Section 7.9 of the Agreement. ICANN and the DPS Working Group will consider the public comments submitted on the agreed DPS Proposed Revisions during such DPS Revisions Posting Period (including comments submitted by the Applicable DPS Parties). Within sixty (60) days of the conclusion of the DPS Revisions Posting Period, the DPS Proposed Revisions (with modifications, if any, to reflect and/or address input from ICANN, the DPS Working Group, and public comments (as applicable)) shall be submitted for DPS Working Group Approval and approval by the ICANN Board of Directors. If such approvals are obtained, the DPS Proposed Revisions shall be deemed an Approved DPS Amendment by the Applicable DPS Parties and ICANN, and shall be effective and deemed an amendment to this Data Processing Specification upon sixty (60) calendar days' notice from ICANN to the Applicable DPS Parties.

13.6.5. If ICANN and the DPS Working Group have not resolved the dispute for any reason by the date that is ninety (90) calendar days following delivery of the DPS Mediation Notice pursuant to Section 13.6, the mediation shall automatically terminate (unless extended by agreement of the parties).

13.7. If, following mediation, ICANN and the DPS Working Group have not reached an agreement on the DPS Proposed Revisions, either the CEO or the DPS Chair may provide the other person written notice (an "Arbitration Notice") requiring ICANN and the Applicable DPS Parties to resolve the dispute through binding arbitration in accordance with the arbitration provisions of Section 5.2 of the Agreement, subject to the requirements and limitations of this Section 13.7.

13.7.1. If an Arbitration Notice is sent, the DPS Proposed Revisions (be those from ICANN, the Working Group, or both) subject to the arbitration shall be posted on ICANN's website for a period of no less than thirty (30) calendar days. The DPS Proposed Revisions, as revised by a party in its discretion, shall be provided to a three (3) person arbitrator panel. For the avoidance of doubt, each party has the right to modify its DPS Proposed Revisions before its submission to the arbitration panel. The arbitration proceeding may not commence prior to the above thirty (30)

calendar day period, and ICANN may consolidate all challenges brought by individual registry operators and registrars into a single proceeding.

13.7.2. Except as set forth in this Section 13.7.2, the arbitration panel shall be selected, and the arbitration proceedings shall be established and conducted, as provided in Section 5.2 of the Agreement.

13.7.3. No amendment to this Data Processing Specification relating to the DPS Proposed Revisions may be submitted for arbitration by either the DPS Working Group or ICANN, unless, in the case of the DPS Working Group, the proposed amendment has received DPS Working Group Approval and, in the case of ICANN, the proposed amendment has been approved by the ICANN Board of Directors.

13.7.4. In order for the arbitrator panel to approve either ICANN or the DPS Working Group's proposed amendment relating to the DPS Proposed Revisions, the arbitrator panel must conclude that such proposed amendment is consistent with a balanced application of the Applicable Data Protection Laws, ICANN's applicable core values (as described in ICANN's Bylaws), and reasonable in light of the balancing of the costs and benefits to the business interests of the Applicable DPS Parties and ICANN (as applicable), and the interests or fundamental rights and freedoms of the Data Subjects which require protection of Personal Data and are to be appropriately considered by the DPS Proposed Revisions as set forth in such amendment. If the arbitrator panel concludes that either ICANN or the DPS Working Group's DPS Proposed Revisions meets the foregoing standard, such amendment shall be effective and deemed an amendment to the Data Processing Specifications upon sixty (60) calendar days' notice from ICANN to Applicable DPS Parties.

13.8. Notwithstanding any other provision of this Data Processing Specification, the DPS Working Group shall be formed, and the DPS Chair shall be appointed, within thirty (30) calendar days of the written request (which may be delivered through electronic means) of ICANN to the chairperson of the Registry Stakeholder Group and the chairperson of the Registrar Stakeholder Group requesting formation of the DPS Working Group and appointment of the DPS Chair. If the DPS Working Group is not formed or the DPS Chair is not appointed within such thirty (30) day period, ICANN may in its sole discretion, upon notice to the chairperson of the Registries Stakeholder Group and the chairperson of the Registrar Stakeholder Group, terminate this Data Processing Specification effective immediately upon delivery of such notice in accordance with the terms of the Agreement.

13.9. Nothing in this Section 13 shall restrict ICANN and Registry Operator from entering into bilateral amendments, modifications, or request for waivers to this Data Processing Specification negotiated solely between the two parties in

accordance with Section 7.6(i) of the Agreement, provided, however, that notwithstanding anything to the contrary in Section 7.6(i) of the Agreement, the Registry Operator can initiate bilateral discussions under Section 7.6(i) of the Agreement only under the following conditions:

13.9.1. It is based on the receipt of either (i) a written legal opinion from a nationally recognized law firm in the applicable jurisdiction that states that compliance with this Data Processing Specification by the Registry Operator is reasonably likely to violate applicable law (the "Opinion"), or (ii) a ruling of, or written guidance from, a governmental body of competent jurisdiction providing that compliance with the Data Processing Specification violates applicable law, the Registry Operator determines in good faith that such compliance violates applicable law, and the Registry Operator provides written notice of such determination to ICANN.

13.9.2. The written notice specifies either (i) a waiver request from compliance with specific terms and conditions of this Data Processing Specification, or (ii) initiation of bilateral amendment discussions pursuant to Section 7.6(i) of the Agreement, (a "DPS Exemption Request"). Such written notice shall: (i) specify the relevant applicable law, the allegedly offending Data Processing Specification terms, the manner in which such terms violates applicable law, and a reasonable description of such determination and any other facts and circumstances related thereto, (ii) be accompanied by a copy of the Opinion and/or governmental ruling or guidance, as applicable, and (iii) be accompanied by any documentation received by the Registry Operator from any governmental authority in each case, related to such determination, and such other documentation reasonably requested by ICANN.

13.9.3. Following receipt of such notice, ICANN and the Registry Operator shall discuss the matter in good faith in an effort to reach a mutually acceptable resolution of the matter. ICANN's office of general counsel may either (i) temporarily or permanently suspend compliance and enforcement of the affected provisions of this Data Processing Specification and grant a waiver under the DPS Exemption Request, or (ii) initiate amendment discussions in accordance with Section 7.6(i) of the Agreement. Prior to granting any waiver or entering into an amendment, ICANN will post its determination on its website for a period of thirty (30) calendar days.

13.9.4. ICANN may, in its discretion, elect to issue a DPS Negotiation Notice to the DPS Chair concerning the DPS Exemption Request. Upon such notice, the parties agree to stop bilateral discussions under the Agreement and follow the negotiation process set forth in this Section 13 of the Data Processing Specification.

14. CONFIDENTIALITY

Any information that a party discloses to the other party (the "receiving party") pursuant to this Data Processing Specification that has been designated in writing to the receiving party as "confidential trade secret," "confidential commercial information," or "confidential financial information" shall be kept confidential by the receiving party in accordance with Section 7.15 of the Agreement.[1]

IN WITNESS WHEREOF, the parties hereto have caused this Data Processing Specification to be executed by their duly authorized representatives as of the effective date first stated above.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

By: _____
Name: _____
Title: _____

[REGISTRY OPERATOR]

By: _____
Name: _____
Title: _____

[1] **ICANN org Note to Draft:** For Registry Agreements that do not contain a relevant confidentiality provision, Section 7.15 of the base gTLD registry agreement will be added to this Data Processing Specification.

ANNEX 1: FACTUAL CIRCUMSTANCES OF PROCESSING

1. Introduction

1.1. This Annex to this Data Processing Specification describes the parties' Processing of Personal Registration Data.

1.2. The Processing described below is performed pursuant to registrar accreditation agreements ("RAAs"), registry agreements ("RAs"), and the Registration Data Policy.

1.3. There are three (3) main categories of Processing contemplated in RAAs, RAs, and the Registration Data Policy:

1.3.1. Personal Registration Data Processing;

1.3.2. Compliance Personal Registration Data Processing; and

1.3.3. Escrowed Personal Registration Data Processing.

1.4. The specific Processing operations performed in each category are described in Section 3 of this Annex (Description of Processing).

2. Types of Personal Data to Be Processed

2.1. Data Subjects may provide Personal Registration Data in connection with the registration of a domain name from a registrar, as specified in Section 2.4 of this Annex.

2.2. Registration Data may or may not contain Personal Data, depending on the individual circumstances of a specific domain name registration.

2.3. The categories of Processing of Personal Registration Data referenced in Section 1.3 of this Annex and described in Section 3 of this Annex each concern the same data element values listed in Section 2.4 of this Annex.

2.4. Personal Registration Data Processed within the scope of this Data Processing Specification and this Annex will include the following data element values. Some of these data values are optional and are not required to be Processed pursuant to RAAs, RAs, and the Registration Data Policy. Also, these values do not include any data a party may Process outside of the scope of RAAs, RAs, and the Registration Data Policy (i.e., in connection with internal business operations):

2.4.1. Domain Name;

2.4.2. Registry Domain ID;

2.4.3. Registrar Whois Server;

2.4.4. Registrar URL;

2.4.5. Updated Date;

2.4.6. Creation Date;

2.4.7. Registry Expiry Date;

2.4.8. Registrar Registration Expiration Date;

2.4.9. Registrar;

2.4.10. Registrar IANA ID;

2.4.11. Registrar Abuse Contact Email;

2.4.12. Registrar Abuse Contact Phone;

2.4.13. Reseller;

2.4.14. Domain Status(es);

2.4.15. Registry Registrant ID;

2.4.16. Registrant Name;

2.4.17. Registrant Organization;

2.4.18. Registrant Street;

2.4.19. Registrant City;

2.4.20. Registrant State/Province;

2.4.21. Registrant Postal Code;

2.4.22. Registrant Phone;

2.4.23. Registrant Phone ext;

2.4.24. Registrant Fax;

2.4.25. Registrant Fax ext;

2.4.26. Registrant Email;

2.4.27. Tech ID;

2.4.28. Tech Name;

2.4.29. Tech Phone; and

2.4.30. Tech Email.

3. Description of Processing

DESCRIPTION OF PROCESSING			
Processing **Category**	**Registry Operator**	**Registrar**	**ICANN**
3.1. Personal Registration Data Processing.	3.1.1.1. Registry Operators receive Personal Registration Data from Registrars. 3.1.1.2. Registry Operators transfer Personal Registration Data to Uniform Rapid Suspension providers. 3.1.1.3. Registry Operators publish Personal Registration Data in the Registration Data Directory Services. 3.1.1.4. Registry Operators transfer Personal Registration Data to third-party requestors. 3.1.1.5. Registry Operators transfer Personal Registration Data to ICANN for	3.1.2.1. Registrars collect Personal Registration Data from registrants. 3.1.2.2. Registrars validate and verify data element values contained in Personal Registration Data. 3.1.2.3. Registrars transfer Personal Registration Data to the Registry Operator. 3.1.2.4 Registrars retain Personal Registration Data. 3.1.2.5. Registrars transfer Personal Registration Data to Uniform Rapid Suspension providers.	3.1.3. ICANN Processes Personal Registration Data from Registry Operators to verify and ensure the operational stability of Registry Services.

Processing **Category**	**Registry Operator**	**Registrar**	**ICANN**
	ICANN to verify and ensure the operational stability of Registry Services.	3.1.2.6. Registrars transfer Personal Registration Data to Uniform Domain Name Dispute Resolution Providers. 3.1.2.7. Registrars publish Personal Registration Data in the Registration Data Directory Services. 3.1.2.8. Registrars transfer Personal Registration Data to third-party requestors.	
3.2 Compliance Personal Registration Data Processing.	3.2.1.1 Registry Operators transfer compliance Personal Registration Data to ICANN, or its designee, for the purposes of responding to an inquiry, notice, or complaint or cooperating with a contractual compliance audit. 3.2.1.2. Registry Operators transfer compliance Personal Registration Data to ICANN, or its designee, to facilitate compliance checks	3.2.2. Registrars transfer compliance Personal Registration Data to ICANN, or its designee, for the purposes of responding to an inquiry, notice, or complaint or cooperating with a contractual compliance audit.	3.2.3.1. ICANN Processes compliance Personal Registration Data in furtherance of its Contractual Compliance function. 3.2.3.2. ICANN Processes compliance Personal Registration Data in the course of auditing a contracted party's compliance with RAA or RA Requirements.

Processing **Category**	**Registry Operator**	**Registrar**	**ICANN**
	on accredited registrars.		
3.3. Escrowed Personal Registration Data Processing.	3.3.1. Registry Operators transfer escrowed Personal Registration Data to an ICANN-approved data escrow agent.	3.3.2. Registrars transfer escrowed Personal Registration Data to an ICANN approved data escrow agent.	3.3.3.1. ICANN Processes escrowed Personal Registration Data in connection with an event requiring Emergency Back End Registry Operator ("EBERO") services. 3.3.3.2. ICANN Processes escrowed Personal Registration Data in connection with a registrar de-accreditation.

ANNEX 2: STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.5(e) and Clause 8.9(b);

(iii) (intentionally left blank)

(iv) Clause 12(a) and (d);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the

data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible

risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

(Intentionally left blank)

Clause 10

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers

and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination - including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data

exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(f) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(g) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(h) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of (specify Member State).[2]

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

[2] **ICANN org note to draft:** ICANN org suggests Belgium because ICANN has establishment in Belgium.

(b) The Parties agree that those shall be the courts of (specify Member State).[3]

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

[3] **ICANN org note to draft**: Should be the jurisdiction whose law is governing the SCCs under Clause 17.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.[4]

[4] **ICANN org note to draft**: Explanatory Note can be deleted, once the SCCs have been completed.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: [Registry Operator]

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): Controller

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: [Internet Corporation for Assigned Names and Numbers]

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

A. Categories of data subjects whose personal data is transferred

Natural person(s) whose Personal Registration Data have been collected pursuant to the Registration Data Policy or the Agreement in connection with a Registered Name.

B. Categories of personal data transferred

Personal Registration Data as defined in Section 1.6 of this Data Processing Specification and including the data element values specified in Section 2.4 of Annex 1 to this Data Processing Specification:

- Domain Name;
- Registry Domain ID;
- Registrar Whois Server;
- Registrar URL;
- Updated Date;
- Creation Date;
- Registry Expiry Date;
- Registrar Registration Expiration Date;
- Registrar;
- Registrar IANA ID;
- Registrar Abuse Contact Email;
- Registrar Abuse Contact Phone;
- Reseller;
- Domain Status(es);
- Registry Registrant ID;
- Registrant Name;
- Registrant Organization;
- Registrant Street;
- Registrant City;
- Registrant State/Province;
- Registrant Postal Code;
- Registrant Phone;

- Registrant Phone ext;
- Registrant Fax;
- Registrant Fax ext;
- Registrant Email;
- Tech ID;
- Tech Name;
- Tech Phone; and
- Tech Email.

C. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

D. The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

Continuous basis depending on rights and obligations stipulated in the Agreement.

E. Nature of the processing

The nature of the Processing is performing the rights and obligations stipulated in the Agreement.

F. Purpose(s) of the data transfer and further processing

- ICANN Processes Personal Registration Data received from Registry Operators to verify and ensure the operational stability of Registry Services.

- ICANN Processes compliance Personal Registration Data received from Registry Operators in furtherance of its Contractual Compliance function.

- ICANN Processes compliance Personal Registration Data received from Registry Operators in the course of auditing a contracted party's compliance with RAA or RA Requirements.

G. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

ICANN will retain Personal Registration Data as stipulated in Section 8 of this Data Processing Specification:

Only (i) as necessary to carry out the Purposes or otherwise in accordance with ICANN Consensus Policies or Temporary Policies and the Agreement, and (ii) as permitted under Applicable Data Protection Laws. If, at any time, any of the foregoing clauses (i) or (ii) is not satisfied, ICANN must promptly delete or return all Personal Registration Data, unless further Processing is permitted under Applicable Data Protection Laws.

H. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:[5]

[insert URL linking to list of ICANN processors for Personal Registration Data]

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Please see section 2.3 of Annex IIIIII.

[5] **Drafting note**: ICANN org plans to create a webpage where processors can be listed. Link to be added before DPS is executed.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

See Section 5 Data Processing Specification (SECURITY OF PERSONAL REGISTRATION DATA).

ANNEX III: ADDITIONAL OPERATIVE PROVISIONS FOR THE IMPLEMENTATION OF STANDARD CONTRACTUAL CLAUSES

1. Introduction

1.1. This Annex to this Data Processing Specification sets out operative provisions for the implementation of the SCCs C-t-C in Annex 2.

1.2. Abbreviations and capitalized terms in this Annex shall have the meaning given to them in the Data Processing Specification.

2. Additional Operative Provisions to the SCCs C-t-C

2.1. **Docking Clause.** Clause 7 ("Docking Clause") of the SCCs C-t-C shall not be included.

2.2. **Redress**. Clause 11 (a) of the SCCs C-t-C shall not include the optional wording on lodging a complaint with an independent dispute resolution body.

2.3. **Supervision.** Clause 13 (a) of the SCCs C-t-C shall apply as follows:

2.3.1. Where the party acting as data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by this party with the GDPR as regards the data transfer shall act as competent Data Protection Authority.

2.3.2. Where the party acting as data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) GDPR, the supervisory authority of the EU Member State in which the representative within the meaning of Article 27(1) GDPR is established shall act as competent Data Protection Authority.

2.3.3. Where the party acting as data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without, however, having to appoint a representative pursuant to Article 27(2) GDPR, the Belgian Data Protection Authority shall act as competent Data Protection Authority.

2.3.4. Where the party acting as data exporter is established in the UK or falls within the territorial scope of UK Applicable Data Protection Laws, the Information Commissioner's Office shall act as competent Data Protection Authority insofar as the relevant data transfer is (also) governed by UK Applicable Data Protection Laws.

2.3.5. Where the party acting as data exporter is established in Switzerland or falls within the territorial scope of Swiss Applicable Data Protection Laws, the Swiss Federal Data Protection and Information Commissioner shall act as competent Data Protection Authority insofar as the relevant data transfer is (also) governed by Swiss Applicable Data Protection Laws.

2.4. **Notification of Government Access Requests.** For the purposes of clause 15(1)(a) of the SCCs C-t-C, the party acting as data importer shall notify the party acting as data exporter (only) and not the Data Subject(s) in each and every case it either:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of Personal Data transferred pursuant to the SCCs C-t-C; or

(ii) becomes aware of any direct access by public authorities to Personal Data transferred pursuant to the SCCs C-t-C in accordance with the laws of the country of destination.

The party acting as data exporter shall be solely responsible for promptly notifying the Data Subject(s) as necessary.

2.5. **Governing law.** The governing law for the purposes of clause 17 of the SCCs C-t-C shall be the law that applies to the Agreement under the rules and principles of conflict of laws. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either

(i) the laws of Belgium; or

(ii) where the Agreement is governed by the laws of the UK, the laws of the UK.

2.6. **Choice of forum and jurisdiction.** The parties agree that the courts under clause 18(b) of the SCCs C-t-C of either:

(i) Belgium; or

(ii) where the Agreement is governed by the laws of the UK, the UK;

shall have exclusive jurisdiction to resolve any dispute arising from the SCCs C-t-C.

3. Data Exports from the UK and Switzerland under the SCCs C-t-C

3.1. **Data Exports from Switzerland under the SCCs C-t-C.** In case of any transfers of Personal Registration Data governed by Applicable Data Protection Laws of Switzerland, the parties agree that the SCCs C-t-C will apply to such transfers in

accordance with section 2 of this Annex III as further specified below in this section:

3.1.1. General and specific references in the SCCs C-t-C to the GDPR, EU or EU Member State law shall have the same meaning as the equivalent reference in the Applicable Data Protection Laws of Switzerland;

3.1.2. For the purposes of Clause 18 (b) of the SCCs C-t-C, the courts of Switzerland shall have exclusive jurisdiction to resolve any dispute arising from the SCCs C-t-C as specified in this section 3.1.;

3.1.3. For the purposes of Clause 18 (c) of the SCCs C-t-C, the term "Member State" shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland); and

3.1.4. The SCCs C-t-C also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Applicable Data Protection Laws of Switzerland until such laws are amended to no longer apply to a legal entity.

3.2. **Data Exports from UK under the SCCs C-t-C**. In case of any transfers of Personal Registration Data governed by the UK GDPR (as defined by the Data Protection Act 2018), the parties hereby enter into the ICO UK Addendum and its alternative part 2 mandatory clauses, which shall form an integral part of this Data Processing Specification. For reference, the ICO UK Addendum is available at the following link: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf or any subsequent link published by the ICO. The parties agree that the SCCs C-t-C apply to such transfers in accordance with section 2 of this Annex III and as amended by the mandatory clauses of the ICO UK Addendum. In accordance with section 17 of the ICO UK Addendum, the parties agree to provide the information set out in part 1 of the ICO UK Addendum in the following format and as further specified below in this section:

3.2.1. The "start date" for the purposes of part 1 of the ICO UK Addendum is the effective date of this Data Processing Specification;

3.2.2. "The parties" for the purposes of part 1 of the ICO UK Addendum are the data exporter listed in Annex I.A in its role as controller and the data importer listed in Annex I.A in its role as controller.

3.2.3. The "key contacts" for the purposes of part 1 of the ICO UK Addendum for the data exporter and the data importer are the person specified in Annex I.A.

3.2.4. The "Addendum SCCs" for the purposes of part 1 of the ICO UK Addendum are the SCCs C-t-C as specified in section 2 of this Annex III;

3.2.5. The "Appendix Information" for the purposes of part 1 of the ICO UK Addendum is the information included in Annex I.A, Annex I.B and Annex II.

3.2.6. For the purposes of part 1 of the ICO UK Addendum, the data importer may end the ICO UK Addendum under the conditions set out in section 19 of the ICO UK Addendum.

* * *