PUBLIC INTEREST REGISTRY

Registry-Registrar Agreement

This Registry-Registrar Agreement (the "Agreement"), dated as of _____ , is made and entered into by and between Public Interest Registry, a Pennsylvania non-profit corporation with its principal place of business located at 11911 Freedom Drive, Suite 1000, 10th Floor, Reston, VA 20190 ("PIR" or the "Registry"), and _____, an Internet Corporation for Assigned Names and Numbers ("ICANN") accredited registrar ("Registrar"). PIR and Registrar may be referred to individually as a "Party" and collectively as the "Parties".

PIR is a party to, or has applied for, a Registry Agreement (each a "Registry Agreement") with ICANN to operate and manage the generic top-level domain names set forth in Schedule A (collectively, the "PIR TLDs," or singularly, a "PIR TLD").

This Agreement shall apply to and govern the Parties' obligations related to the registration of domain names and provision of services to the Registrar through the Registry System for each PIR TLD that Registrar elects to offer to its customers. For the avoidance of doubt, Registrar shall be responsible for the maintenance of all domain names in each PIR TLD registered through its systems even if Registrar elects to discontinue new registrations in such PIR TLD. By signing this Agreement, Registrar is permitted, but not obligated, to offer for registration each of the TLDs listed on Schedule A. Similarly, if PIR is not the Registry Operator for any of the TLDs listed on Schedule A (if an assignment for any of the TLDs is not effectuated or for any other reason) the terms of this Agreement shall not apply to those TLDs.

1. DEFINITIONS

1.1. The "APIs" are the application program interfaces by which Registrar may interact, through the EPP, with the Registry System.

1.2. "Confidential Information" means all information and materials, including, without limitation, computer software, data, information, intellectual property, databases, protocols, reference implementation and documentation, financial information, statistics, and functional and interface specifications, provided by the Disclosing Party to the Receiving Party under this Agreement and marked or otherwise identified as Confidential, provided that if a communication is oral, the Disclosing Party will notify the Receiving Party in writing, including by email, within fifteen (15) days of the disclosure that it is confidential.

1.3. "DNS" means the Internet domain name system.

1.4. The "Effective Date" shall be the date set forth above.

1.5. "EPP" means the Extensible Provisioning Protocol, which is the protocol used by the Registry System.

1.6. "ICANN" means the Internet Corporation for Assigned Names and Numbers.

1.7. "Personal Data" has the meaning as set forth in Exhibit 1: RRA Data Processing Addendum.

1.8. "Registered Name" refers to a domain name within one of the PIR TLDs, whether consisting of two or more levels, about which PIR or an affiliate engaged in providing Registry Services maintains data in a Registry Database, arranges for such maintenance, or derives revenue from such maintenance. A name in a Registry Database may be a Registered Name even though it does not appear in a TLD zone file (e.g., a registered but inactive name).

1.9. "Registered Name Holder" means the holder of a Registered Name.

1.10. "Registry Agreement" shall have the meaning set forth in the Preamble of this Agreement.

1.11. "Registry Database" means a database comprised of data about one or more domain name registrations within PIR TLDs.

1.12. "Registry Policies" means the policies adopted and updated from time to time pursuant to Section 3.5.2 below by the Registry and posted under "Policies" on the Registry Website.

1.13. "Registry Services" has the meaning set forth in the Registry Agreement.

1.14. The "Registry System" means the system operated by PIR, or contractors on behalf of PIR, for Registered Names in the PIR TLDs.

1.15. The "Registry Website" means PIR's website www.pir.org. If this Registry Website address changes, PIR will provide Registrar with at least thirty (30) days' notice pursuant to Section 3.5.2.

1.16. "Term" means the term of this Agreement, as set forth in this Agreement.

1.17. A "TLD" means a top-level domain of the DNS delegated by ICANN.

1.18. "TLD Specific Terms" means any obligations, terms, or conditions that are only applicable to one or more, but not all, PIR TLDs. Such terms are set forth in Schedule B and are only applicable to the TLDs specifically referenced therein.

Other terms used in this Agreement as defined terms shall have the meanings ascribed to them in the context in which they are defined.

2. OBLIGATIONS OF PIR

2.1. Access to Registry System. Throughout the Term of this Agreement, PIR, or contractors on its behalf, shall operate the Registry System and provide Registrar with access to the Registry System to transact domain name registration information for domain names within the PIR TLDs to the Registry System. To obtain such access, PIR may require Registrar to successfully complete operation testing in an Operational Test and Evaluation environment made available by PIR or its contractors. Nothing in this Agreement entitles Registrar to enforce any agreement between PIR and ICANN.

2.2. Maintenance of Registrations Sponsored by Registrar. Subject to the provisions of this Agreement, and Registrar's Accreditation Agreement with ICANN, PIR shall maintain the registrations of Registered Names sponsored by Registrar in the Registry System during the term for which Registrar has paid the fees required by this Agreement.

2.3. Provision of Technical Specifications; License. PIR shall provide Registrar with the technical specifications to permit Registrar to interface with the Registry System. Subject to the terms of this Agreement, PIR grants, and Registrar accepts a non-exclusive, non-transferable, worldwide limited license to access the Registry System, including any applicable updates and upgrades thereto in order to provide domain name registration services in the PIR TLDs only and for no other purpose.

2.4. Changes to System. PIR may from time to time modify, revise, or augment the features of the Registry System at its sole discretion. PIR will provide Registrar with at least ninety (90) days' notice prior to the implementation of any material changes to the Registry System.

2.5. Engineering and Customer Service Support.

2.5.1. Engineering Support. PIR agrees to provide Registrar with reasonable engineering telephone support (24 hour/7 day) to address engineering issues arising in connection with Registrar's use of the Registry System.

2.5.2. Customer Service Support. During the Term of this Agreement, PIR will provide reasonable telephone and e-mail customer service support to Registrar (but not to Registered Name Holders or prospective customers of Registrar), for non-technical issues solely relating to the Registry System and its operation. PIR will provide Registrar with a telephone number and e-mail address for such support during implementation of the Protocol and APIs. First-level telephone support will be available on business days between the hours of 9 a.m. and 5 p.m. Eastern US time.

2.6. ICANN Requirements. PIR's obligations hereunder are subject to modification at any time as the result of ICANN-mandated requirements and consensus policies. Notwithstanding anything in this Agreement to the contrary, Registrar shall comply with any such ICANN requirements in accordance with the timeline defined by ICANN.

2.7. Integrity, Stability and Security; Mitigation Processes. PIR shall use commercially reasonable efforts to preserve the stability and security of, and confidence in, the PIR TLDs and the DNS in general for the benefit of the entire Internet community. Registrar acknowledges and agrees that PIR reserves the right to deny, suspend, cancel, or transfer any registration or transaction, or place any Registered Name(s) on registry lock, hold or similar status, that it deems necessary, in its sole discretion; (a) to protect the integrity and stability of the registry; (b) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or as needed during or following any dispute resolution process; (c) to comply with the terms of the Registry Agreement; (d) if the domain name use violates PIR's Anti-Abuse Policy or other PIR policies applicable to the relevant TLD, including TLD Specific Policies; (e) to avoid any liability, civil or criminal, on the part of PIR, as well as its affiliates, subsidiaries, officers, directors, and employees; (f) per the terms of the Registration Agreement; or (g) to correct mistakes made by PIR or any registrar in connection with a domain name registration. If PIR makes any such change to any domain name(s), PIR will notify

Registrar via EPP poll message, except when such notice would contravene existing law, applicable technical standards, or this Agreement.

3. OBLIGATIONS OF REGISTRAR

3.1. Accredited Registrar. During the Term of this Agreement, Registrar shall maintain in full force and effect its ICANN accreditation.

3.2. Registrar Responsibility for Customer Support and Abuse Mitigation.

3.2.1. Registrar shall be responsible for providing all customer and technical support to Registered Name Holders in each of the PIR TLDs. This includes all customer, technical, and billing support related to the registration, modification, renewal, transfer, and deletion of domain names under its sponsorship.

3.2.2. Registrar shall maintain an abuse point of contact in accordance with its Registrar Accreditation Agreement with ICANN that can be contacted where incidents of abusive activities as defined by ICANN, PIR's Anti-Abuse Policy, or any other applicable Registry Policy is suspected, or has been found, by PIR.

3.2.3. Registrar shall have processes in place to appropriately address reports of abusive activities as defined by ICANN, PIR's Anti-Abuse Policy, or any other applicable Registry Policy and have systems in place to reasonably mitigate such abuse. Registrar acknowledges and agrees that PIR reserves the right to take any action on abusive Registered Names as set forth in such policies.

3.3. Registrar's Registration Agreement. At all times while it is sponsoring the registration of any Registered Name within the Registry System, Registrar shall have in effect an electronic or paper registration agreement with the Registered Name Holder. Registrar shall include in its registration agreement those terms required by this Agreement, its Registrar Accreditation Agreement with ICANN, and other terms that are consistent with Registrar's obligations to PIR under this Agreement.

3.4. Indemnification Required of Registered Name Holders. In its registration agreement with each Registered Name Holder, Registrar shall require such Registered Name Holder to indemnify, defend, and hold harmless PIR and its subcontractors, and the directors, officers, employees, affiliates, and agents of each of them, from and against all claims, damages, liabilities, costs and expenses, including reasonable legal fees and expenses, arising out of or relating to the Registered Name Holder's domain name registration. The registration agreement shall further require that this indemnification obligation survive the termination or expiration of the registration agreement.

3.5. Compliance with Terms and Conditions. Registrar shall comply with each of the following requirements, and further shall include in its registration agreement with each Registered Name Holder an obligation for such Registered Name Holder to comply with each of the following requirements:

3.5.1. ICANN standards, policies, procedures, and practices for which Registrar or PIR has in accordance with the Registry Agreement, the Registrar Accreditation Agreement, or other arrangement with ICANN; and

3.5.2. operational standards, policies, procedures, and practices for PIR TLDs established from time to time by PIR in a non-arbitrary manner and applicable to all registrars, including any applicable affiliate(s) or contractor(s) of PIR, and consistent with ICANN's standards, policies, procedures, and practices and PIR's relevant Registry Agreements with ICANN. Additional or revised PIR operational standards, policies, procedures, and practices for PIR TLDs shall be effective upon thirty (30) days' notice by PIR to Registrar. If there is a discrepancy between the terms required by this Agreement and the terms of the Registrar's registration agreement, the terms of this Agreement shall supersede those of the Registrar's registration agreement.

3.6. Additional Requirements for Registration Agreement. In addition to the provisions of this Subsection, in its registration agreement with each Registered Name Holder, Registrar shall require such Registered Name Holder to:

3.6.1. consent to the use, copying, distribution, publication, transfer, modification, and other processing of Registered Name Holder's Personal Data by PIR and its designees and agents in a manner consistent with the purposes specified pursuant to Exhibit 1, RRA Data Processing Addendum.

3.6.2. submit to proceedings commenced under ICANN's Uniform Domain Name Dispute Resolution Policy ("UDRP");

3.6.3. submit to proceedings commenced under ICANN's Uniform Rapid Suspension ("URS") process;

3.6.4. immediately correct and update the registration information for the Registered Name during the registration term for the Registered Name;

3.6.5. agree to be bound by any TLD Specific Terms as set forth in Schedule B, TLD Specific Terms, for the applicable PIR TLDs Registrar offers for registration;

3.6.6. if Registrar participates in the initial launch of any of the PIR TLDs, agree to be bound by the terms of such, including without limitation the sunrise period and the land rush period, and the Sunrise Dispute Resolution Policy, and further to acknowledge that PIR has no liability of any kind for any loss or liability resulting from the proceedings and processes relating to the sunrise period or the land rush period, including, without limitation: (a) the ability or inability of a registrant to obtain a Registered Name during these periods and (b) the results of any dispute over a sunrise registration;

3.6.7. agree not to distribute malware, abusively operate botnets, phishing, piracy, trademark, or copyright infringement, fraudulent or deceptive practices, counterfeiting, or otherwise engaging in activity contrary to PIR's Anti-Abuse Policy, or other PIR Policies applicable to the particular PIR TLD, or applicable law; and

3.6.8. acknowledge and agree that PIR reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that it deems necessary, in its discretion; (1) to protect the integrity and stability of the Registry Database or the Registry System; (2) to comply with any applicable laws, government rules or requirements, requests

of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of PIR, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement (5) pursuant to PIR's Anti-Abuse Policy or other PIR policies applicable to the relevant TLD; or (6) to correct mistakes made by PIR or any Registrar in connection with a Registered Name. PIR also reserves the right to place upon registry lock, hold, or similar status a domain name during resolution of a dispute.

3.7. Data Submission Requirements.

3.7.1. As part of its registration and sponsorship of Registered Names in PIR TLDs, Registrar shall submit complete data as required by technical specifications of the Registry System that are made available to Registrar from time to time. Registrar hereby grants PIR a non-exclusive, non-transferable, limited license to such data for propagation of and the provision of authorized access to the TLD zone files and as otherwise required in PIR's operation of PIR TLDs.

3.7.2. Registrar shall submit any corrections or updates from a Registered Name Holder relating to the registration information for a Registered Name to PIR in a timely manner.

3.8. Security.

3.8.1. Registrar shall develop and employ in its domain name registration business all necessary technology and restrictions to ensure that its connection to the Registry System is secure and that all data exchanged between Registrar's system and the Registry System shall be protected to avoid unintended disclosure of information. Registrar shall employ the necessary measures to prevent its access to the Registry System granted hereunder from being used to (i) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than its own existing customers; or (ii) enable high volume, automated, electronic processes that send queries or data to the systems of PIR, any other registry operated under an agreement with ICANN, or any ICANN-accredited registrar, except as reasonably necessary to register domain names or modify existing registrations. In addition, PIR may require other reasonable security provisions to ensure that the Registry System is secure and stable.

3.8.2. The Registrar shall provide the Registered Name Holder with timely access to the authorization code along with the ability to modify the authorization code. Registrar shall respond to any inquiry by a Registered Name Holder regarding access to or modification of an authorization code within five (5) calendar days.

3.9. Resolution of Technical Problems. Registrar shall employ necessary employees, contractors, or agents with sufficient technical training and experience to respond to and fix all technical problems concerning the use of the EPP, the APIs, and the systems of PIR in conjunction with Registrar's systems. In the event of significant degradation of the Registry System or other emergency, PIR may, in its sole discretion, temporarily suspend or restrict Registrar's access to the Registry System. Such temporary suspensions shall be applied in a non-arbitrary manner and shall apply fairly to any registrar similarly situated, including affiliates of PIR.

3.10. Time. In the event of any dispute concerning the time of the entry of a domain name registration into the Registry Database, the time shown in the Registry records shall control.

3.11. Transfer of Registration Sponsorship. Registrar agrees to implement transfers of Registered Name registrations from another registrar to Registrar and vice versa pursuant to the Policy on Transfer of Registrations Between Registrars as may be amended from time to time by ICANN (the "Transfer Policy").

3.12. Restrictions on Registered Names. In addition to complying with ICANN standards, policies, procedures, and practices limiting domain names that may be registered, Registrar agrees to comply with applicable statutes and regulations limiting the domain names that may be registered.

4. FEES

4.1. Amount of PIR Fees. Registrar agrees to pay PIR the fees set forth in Schedule C for services provided by PIR to Registrar (collectively, "Fees"). PIR reserves the right to revise the Standard Fees (as described in Schedule C) from time to time, provided that PIR shall provide at least six (6) months' notice to Registrar prior to any such increases. In addition, Registrar agrees to pay PIR the applicable Variable Fees assessed to Registry Operator by ICANN, as set forth in the applicable Registry Agreements. All payments shall be made in accordance with the processes set forth in Schedule C. PIR reserves the right to modify its billing and collections policies from time to time, provided that PIR shall provide notice of such modifications in accordance with Section 3.5.2.

4.2. Taxes. All Fees due under this Agreement are exclusive of tax. All taxes, duties, fees and other governmental charges of any kind (including sales, turnover, services, use and value-added taxes, but excluding taxes based on the net income of PIR) which are imposed by or under the authority of any government or any political subdivision thereof on the fees for any services, software and/or hardware shall be borne by Registrar and shall not be considered a part of, a deduction from or an offset against such Fees. All payments due to PIR shall be made without any deduction or withholding on account of any tax, duty, charge or penalty except as required by law, in which case, the sum payable by Registrar from which such deduction or withholding is to be made shall be increased to the extent necessary to ensure that, after making such deduction or withholding, PIR receives and retains (free from any liability with respect thereof) a net sum equal to the sum it would have received but for such deduction or withholding being required.

5. CONFIDENTIALITY AND INTELLECTUAL PROPERTY

5.1. Use of Confidential Information. During the Term of this Agreement, each party (the "Disclosing Party") may disclose its Confidential Information to the other party (the "Receiving Party"). Each party's use and disclosure of the Confidential Information of the other party shall be subject to the following terms:

5.1.1. The Receiving Party shall treat as strictly confidential, and use all reasonable efforts to preserve the secrecy and confidentiality of, all Confidential Information of the Disclosing Party, including implementing reasonable physical security measures and operating procedures.

5.1.2. The Receiving Party agrees that it will use any Confidential Information of the Disclosing Party solely for the purpose of exercising its right or performing its obligations under this Agreement and for no other purposes whatsoever.

5.1.3. The Receiving Party shall make no disclosures of any Confidential Information of the Disclosing Party to others; provided, however, that if the Receiving Party is a corporation, partnership, or similar entity, disclosure is permitted to the Receiving Party's officers, employees, contractors and agents who have a demonstrable need to know such Confidential Information, provided the Receiving Party shall advise such personnel of the confidential nature of the Confidential Information and of the procedures required to maintain the confidentiality thereof, and shall require them to acknowledge in writing that they have read, understand, and agree to be individually bound by the confidentiality terms of this Agreement.

5.1.4. The Receiving Party shall not modify or remove any confidentiality legends or copyright notices appearing on any Confidential Information of the Disclosing Party.

5.1.5. The Receiving Party agrees not to prepare any derivative works based on the Confidential Information.

5.1.6. Notwithstanding the foregoing, this Subsection imposes no obligation upon the Parties with respect to information that (i) is disclosed in the absence of a confidentiality agreement and such disclosure was agreed to by the Disclosing Party in writing prior to such disclosure; or (ii) is or has entered the public domain through no fault of the Receiving Party; or (iii) is known by the Receiving Party prior to the time of disclosure; or (iv) is independently developed by the Receiving Party without use of the Confidential Information; or (v) is made generally available by the Disclosing Party without restriction on disclosure; or (vi) is required to be disclosed by law, regulation or court order; provided, that in the event the Receiving Party is required by law, regulation or court order to disclose any of Disclosing Party's Confidential Information, Receiving Party will promptly notify Disclosing Party in writing prior to making any such disclosure in order to facilitate Disclosing Party seeking a protective order or other appropriate remedy from the proper authority, at the Disclosing Party's expense. Receiving Party agrees to cooperate with Disclosing Party in seeking such order or other remedy. Receiving Party further agrees that if Disclosing Party is not successful in precluding the requesting legal body from requiring the disclosure of the Confidential Information, it will furnish only that portion of the Confidential Information which is legally required.

5.1.7. The Receiving Party's duties under this Subsection shall expire two (2) years after the expiration or termination of this Agreement or earlier, upon written agreement of the Parties.

5.2. Intellectual Property.

5.2.1. Subject to the licenses granted hereunder, each party will continue to independently own its intellectual property, including all patents, trademarks, trade names, service marks, copyrights, trade secrets, proprietary processes, and all other forms of intellectual property.

5.2.2. Without limiting the generality of the foregoing, no commercial use rights or any licenses under any patent, patent application, copyright, trademark, know-how, trade secret, or any other intellectual proprietary rights are granted by the Disclosing Party to the Receiving Party by this Agreement, or by any disclosure of any Confidential Information to the Receiving Party under this Agreement.

6. INDEMNITIES AND LIMITATION OF LIABILITY

6.1. Indemnification. Registrar, at its own expense and within thirty (30) days after presentation of a demand by PIR under this Section, will indemnify, defend and hold harmless PIR and its subcontractors, and the directors, officers, employees, representatives, agents, and affiliates of each of them, against any claim, suit, action, or other proceeding brought against any such party(ies) based on or arising from any claim or alleged claim: (i) relating to any product or service of Registrar; (ii) relating to any agreement, including Registrar's dispute policy, with any Registered Name Holder or Registrar; or (iii) relating to Registrar's domain name registration business, including, but not limited to, Registrar's advertising, domain name application process, systems and other processes, fees charged, billing practices, and customer service. PIR shall provide Registrar with prompt notice of any such claim, and upon Registrar's written request, PIR will provide to Registrar all available information and assistance reasonably necessary for Registrar to defend such claim, provided that Registrar reimburses PIR for PIR's actual and reasonable costs incurred in connection with providing such information and assistance. Registrar will not enter into any settlement or compromise of any such indemnifiable claim without PIR's prior written consent, which consent shall not be unreasonably withheld. Registrar will pay any costs, damages, and expenses, including, but not limited to, reasonable attorneys' fees and costs awarded against or otherwise incurred by PIR in connection with or arising from any such indemnifiable claim, suit, action, or proceeding.

6.2. Representation, Warranty, and Covenant. Registrar represents, warrants, and covenants that: (i) it is and will remain a corporation duly incorporated, validly existing and in good standing under the law of the jurisdiction of its formation (ii) it has all requisite corporate power and authority to execute, deliver, and perform its obligations under this Agreement, (iii) the execution, performance and delivery of this Agreement has been duly authorized by Registrar, (iv) it is and will remain in compliance with applicable laws and regulations, (v) it is, and will continue to be, accredited by ICANN or its successor and (vi) no further approval, authorization or consent of any governmental or regulatory authority is required to be obtained or made by Registrar in order for it to enter into and perform its obligations under this Agreement.

6.3. Limitation of Liability. EXCEPT IN CONNECTION WITH A PARTY'S INDEMNITY OR CONFIDENTIALITY OBLIGATIONS HEREUNDER, IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE, EXEMPLARY, OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES RESULTING FROM LOSS OF PROFITS OR BUSINESS INTERRUPTION, ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, EVEN IF THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE MAXIMUM AGGREGATE LIABILITY OF PIR AND ITS SUBCONTRACTORS EXCEED THE LESSER OF (i) THE TOTAL AMOUNT PAID TO PIR UNDER THE TERMS OF THIS AGREEMENT FOR THE IMMEDIATELY PRECEEDING 12 MONTH PERIOD, OR (ii) $100,000 USD.

6.4. Disclaimer of Warranties. THE REGISTRY SYSTEM AND THE PROVISION OF REGISTRY SERVICES AS WELL AS ANY OTHER SERVICES PROVIDED UNDER THIS AGREEMENT ARE PROVIDED "AS-IS" AND WITHOUT ANY WARRANTY OF ANY KIND. PIR EXPRESSLY DISCLAIMS ALL WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR SATISFACTORY QUALITY AND FITNESS FOR

A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD-PARTY RIGHTS. PIR DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE REGISTRY SYSTEM WILL MEET REGISTRAR'S REQUIREMENTS, OR THAT THE OPERATION OF THE REGISTRY SYSTEM WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE REGISTRY SYSTEM WILL BE CORRECTED. FURTHERMORE, PIR DOES NOT WARRANT NOR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE REGISTRY SYSTEM OR RELATED DOCUMENTATION IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. SHOULD THE REGISTRY SYSTEM PROVE DEFECTIVE, REGISTRAR ASSUMES THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION OF REGISTRAR'S OWN SYSTEMS AND SOFTWARE.

7. INSURANCE

7.1. Insurance Requirements. PIR may, at its sole discretion, require Registrar to provide proof of reasonable general liability insurance.

8. DISPUTE RESOLUTION

8.1. Dispute Resolution. Disputes arising under or in connection with this Agreement, including requests for specific performance, shall be resolved through binding arbitration conducted as provided in this Section pursuant to the rules of the American Arbitration Association ("AAA"). The arbitration shall be conducted in the English language and shall occur in Fairfax County, Virginia, United States of America. There shall be three arbitrators: each party shall choose one arbitrator and, if the two arbitrators are not able to agree on a third arbitrator, the third shall be chosen by the AAA. The parties shall bear the costs of the arbitration in equal shares, subject to the right of the arbitrators to reallocate the costs in their award as provided in the AAA rules. The parties shall bear their own attorneys' fees in connection with the arbitration, and the arbitrators may not reallocate the attorneys' fees in conjunction with their award. The arbitrators shall render their decision within ninety (90) days of the initiation of arbitration. Any litigation brought to enforce an arbitration award shall be brought in the state or federal courts of the Commonwealth of Virginia, United States of America; however, the parties shall also have the right to enforce a judgment of such a court in any court of competent jurisdiction. For the purpose of aiding the arbitration or preserving the rights of a party during the pendency of an arbitration, each party shall have the right to seek temporary or preliminary injunctive relief from the arbitration panel or a court located in the state or federal courts in the Commonwealth of Virginia, United States of America, which shall not be a waiver of this arbitration agreement.

9. TERM AND TERMINATION

9.1. Term of the Agreement; Revisions. The Term of this Agreement shall commence on the Effective Date and, unless earlier terminated in accordance with the provisions of this Agreement, shall expire on the last day of the calendar month which is two (2) years following the Effective Date. This Agreement shall automatically renew for additional successive two (2) year terms unless Registrar provides notice of termination to Registry Operator at least thirty (30) days prior to the end of the initial or any renewal term. If revisions to PIR’s approved form of Registry-Registrar Agreement are approved or adopted by ICANN, Registrar will either execute an amendment

substituting the revised agreement in place of this Agreement or, at its option exercised within fifteen (15) days after receiving notice of such amendment, terminate this Agreement immediately by giving written notice to PIR. If PIR does not receive such executed amendment or notice of termination from Registrar within such fifteen (15) day period, Registrar shall be deemed to have terminated this Agreement effective immediately.

9.2. Termination. This Agreement may also be terminated as follows:

9.2.1. Termination For Cause. If either party materially breaches any of its obligations under this Agreement and such breach is not substantially cured within thirty (30) calendar days after written notice thereof is given by the other party, then the non-breaching party may, by giving written notice thereof to the other party, terminate this Agreement as of the date specified in such notice of termination.

9.2.2. Termination at Option of Registrar. Registrar may terminate this Agreement at any time by giving PIR thirty (30) days' notice of termination.

9.2.3. Termination Upon Loss of Registrar's Accreditation. This Agreement shall immediately terminate if Registrar's accreditation by ICANN is terminated or expires without renewal.

9.2.4. Termination in the Event of Termination of all Registry Agreements. This Agreement shall terminate if PIR's Registry Agreements with ICANN are all terminated or expire without entry of a subsequent Registry Agreement with ICANN and this Agreement is not assigned pursuant to the terms herein.

9.2.5. Termination in the Event of Insolvency or Bankruptcy. Either party may terminate this Agreement if the other party is adjudged insolvent or bankrupt, or if proceedings are instituted by or against a party seeking relief, reorganization or arrangement under any laws relating to insolvency, or seeking any assignment for the benefit of creditors, or seeking the appointment of a receiver, liquidator or trustee of a party's property or assets or the liquidation, dissolution or winding up of a party's business.

9.3. Effect of Termination. Upon the expiration or termination of this Agreement for any reason:

9.3.1. PIR will complete the registration of all domain names processed by Registrar prior to the effective date of such expiration or termination, provided that Registrar's payments to PIR for Fees are current and timely.

9.3.2. Registrar shall immediately transfer its sponsorship of Registered Names to another ICANN-accredited registrar in compliance with any procedures established or approved by ICANN.

9.3.3. All Confidential Information of the Disclosing Party in the possession of the Receiving Party shall be immediately returned to the Disclosing Party.

9.3.4. In the event of termination in accordance with the provisions of Subsections 9.1, 9.2.1, 9.2.2, 9.2.3 or 9.2.5, PIR reserves the right to immediately contact all Registered Name Holders to facilitate the orderly and stable transition of Registered Name Holders to other ICANN-accredited registrars.

9.3.5. All Fees owing to PIR shall become immediately due and payable.

9.4. Survival. In the event of termination of this Agreement, the following shall survive: (i) Subsections 3.6, 5.1, 5.2, 6.1, 6.3, 6.4, 8.1, 9.4, 10.2, 10.3, 10.4, 10.6, 10.7, 10.8 and 10.9, (ii) all Schedules and Exhibits, and (iii) the Registered Name Holder's indemnification obligation under Subsection 3.4. Neither party shall be liable to the other for damages of any sort resulting solely from terminating this Agreement in accordance with its terms.

10. MISCELLANEOUS

10.1. Assignments.

10.1.1. Assignment to Successor Registry. In the event the PIR's Registry Agreements are all terminated or expire without entry by PIR and ICANN of a subsequent registry agreement, PIR's rights under this Agreement may be assigned to a company with a subsequent registry agreement covering the PIR TLDs upon ICANN's giving Registrar written notice within sixty (60) days of the termination or expiration, provided that the subsequent PIR assumes the duties of PIR under this Agreement. The terms of this RRA remain in full force and effect so long as PIR maintains the Registry Agreement for at least one of the TLDs on Schedule A.

10.1.2. Assignment in Connection with Assignment of Agreement with ICANN. If PIR's Registry Agreements with ICANN for a particular PIR TLDs is validly assigned, PIR's rights under this Agreement with respect to that TLD shall be automatically assigned to the assignee of the Registry Agreement, provided that the assignee assumes the duties of PIR under this Agreement. If Registrar's Accreditation Agreement with ICANN is validly assigned, Registrar's rights under this Agreement shall be automatically assigned to the assignee of the Registrar Accreditation Agreement, provided that the subsequent registrar assumes the duties of Registrar under this Agreement.

10.1.3. Other Assignments. Except as otherwise expressly provided in this Agreement, the provisions of this Agreement shall inure to the benefit of and be binding upon, the successors, and permitted assigns of the parties. Neither party shall assign or transfer its rights or obligations under this Agreement without the prior written consent of the other party, which shall not be unreasonably withheld.

10.2. Notices. Any notice or other communication required or permitted to be delivered to any Party under this Agreement shall be in writing and shall be deemed properly delivered, given and received when delivered (by hand, by registered mail, by courier or express delivery service, or by e-mail during business hours) to the contact provided by the Registrar:

_____

_____

_____

If to PIR:

Public Interest Registry
11911 Freedom Drive, Suite 1000, 10th Floor
Reston, VA 20190, U.S.A.

Attention: Operations Department
Email: (As specified from time to time.)
with a copy to: legal@pir.org

10.3. Third-Party Beneficiaries. The parties expressly agree that ICANN is an intended third-party beneficiary of this Agreement. Otherwise, this Agreement shall not be construed to create any obligation by either party to any non-party to this Agreement, including any holder of a Registered Name. Registrar expressly acknowledges that, notwithstanding anything in this Agreement to the contrary, it is not an intended third-party beneficiary of the Registry Agreement.

10.4. Relationship of the Parties. Nothing in this Agreement shall be construed as creating an employer-employee or agency relationship, a partnership, or a joint venture between the parties.

10.5. Force Majeure. Neither party shall be liable to the other for any loss or damage resulting from any cause beyond its reasonable control (a "Force Majeure Event") including, but not limited to, insurrection or civil disorder, war or military operations, national or local emergency, acts or omissions of government or other competent authority, compliance with any statutory obligation or executive order, industrial disputes of any kind (whether or not involving either party's employees), fire, lightning, explosion, flood, subsidence, weather of exceptional severity, and acts or omissions of persons for whom neither party is responsible. Upon occurrence of a Force Majeure Event and to the extent such occurrence interferes with either party's performance of this Agreement, such party shall be excused from performance of its obligations (other than payment obligations) during the first six (6) months of such interference, provided that such party uses best efforts to avoid or remove such causes of nonperformance as soon as possible.

10.6. Amendments. No amendment, supplement, or modification of this Agreement or any provision hereof shall be binding unless executed in writing by both parties.

10.7. Waivers. No failure on the part of either party to exercise any power, right, privilege or remedy under this Agreement, and no delay on the part of either party in exercising any power, right, privilege or remedy under this Agreement, shall operate as a waiver of such power, right, privilege, or remedy; and no single or partial exercise or waiver of any such power, right, privilege, or remedy shall preclude any other or further exercise thereof or of any other power, right, privilege or remedy. Neither party shall be deemed to have waived any claim arising out of this Agreement, or any power, right, privilege, or remedy under this Agreement, unless the waiver of such claim, power, right, privilege, or remedy is expressly set forth in a written instrument duly executed and delivered on behalf of such party; and any such waiver shall not be applicable or have any effect except in the specific instance in which it is given.

10.8. Governing Law. This Agreement and its interpretation (including its interpretation by the arbitrators in accordance with the terms of this Agreement) shall be governed by and construed in accordance with the internal laws of the Commonwealth of Virginia, United States of America, in all respects and as applied to agreements entered into among Virginia residents to be performed entirely within Virginia, without giving effect to any choice or conflict of law provision or rule (whether of the Commonwealth of Virginia or any other jurisdiction) that would cause the application of laws of any jurisdictions other than those of Commonwealth of Virginia.

10.9. Entire Agreement. This Agreement (including its Schedules and Exhibits, which form a part of it) constitutes the entire agreement between the parties concerning the subject matter of this Agreement and supersedes any prior agreements, representations, statements, negotiations, understandings, proposals, or undertakings, oral or written, with respect to the subject matter expressly set forth herein.

10.10. Severability. If any provision of this Agreement or the application thereof to any person, entity, or circumstances is determined to be invalid, illegal, or unenforceable in any jurisdiction, the remainder hereof, and the application of such provision to such person, entity, or circumstances in any other jurisdiction, shall not be affected thereby, and to this end the provisions of this Agreement shall be severable.

10.11. Counterparts. All executed copies of this Agreement are duplicate originals, equally admissible as evidence. This Agreement may be executed in counterparts, and such counterparts taken together shall be deemed the Agreement. A facsimile copy of a signature of a party hereto shall have the same effect and validity as an original signature.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the date set forth in the first paragraph hereof.

PUBLIC INTEREST REGISTRY	[Registrar]_____
By: _____	By: _____
Name:_____	Name:_____
Title:_____	Title:_____

Schedule A
PIR TLDs

PIR either serves as the Registry Operator for, or has applied to ICANN to serve as the Registry Operator for, the following TLDs:

.ORG
.NGO
.ONG
.CHARITY
.GIVES
.GIVING
.FOUNDATION
.ОРГ (.xn--c1avg)
.机构 (.xn--nqv7f)
.संगठन (.xn--i1b6b1a6a2e)

For TLDs for which PIR has applied to serve as Registry Operator to ICANN, the terms of this Agreement shall become effective relating to those TLDs upon ICANN's delegation or assignment of the corresponding Registry Agreement to PIR, though such delegation or assignment does not require Registrar to offer registrations in such TLDs.

Schedule B
TLD Specific Terms

.CHARITY TLD Specific Terms

Pursuant to the requirements of Specification 11 of the .CHARITY Registry Agreement, Registrar shall include in its Registration Agreement with each Registered Name Holder in the .CHARITY TLD an obligation for such Registered Name Holder to comply with each of the following additional requirements:

(a) A provision requiring that Registered Name Holders will comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.

(b) A provision requiring that Registered Name Holders who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law.

(c) A provision requiring Registered Name Holders to provide administrative contact information, which must be kept up-to-date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self-regulatory, bodies in their main place of business.

(d) A provision requiring a representation that the Registered Name Holder possesses any necessary authorizations, charters, licenses and/or other related credentials for participation in the sector associated with the TLD.

(e) A provision requiring Registered Name Holders to report any material changes to the validity of the Registered Name Holders' authorizations, charters, licenses and/or other related credentials for participation in the sector associated with the TLD in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve.

.GIVES TLD Specific Terms

Pursuant to the requirements of Specification 11 of the .GIVES Registry Agreement, Registrar shall include in its Registration Agreement with each Registered Name Holder in the .GIVES TLD an obligation for such Registered Name Holder to comply with each of the following additional requirements:

(a) A provision requiring Registered Name Holders to comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.

(b) A provision requiring that Registered Name Holders who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law.

.GIVING TLD Specific Terms

Pursuant to the requirements of Specification 11 of the .GIVING Registry Agreement, Registrar shall include in its Registration Agreement with each Registered Name Holder in the .GIVING TLD an obligation for such Registered Name Holder to comply with each of the following additional requirements:

(a) A provision requiring Registered Name Holders to comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.

(b) A provision requiring that Registered Name Holders who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law.

.NGO and .ONG TLD Specific Terms

As required by Specification 12 of the .NGO and .ONG Registry Agreements, this Agreement relating to registration of names in the .NGO and .ONG TLDs allows only the registration of names that comply with the validation requirements for non-governmental organizations ("NGOs"). When Registrar registers a domain name in the .NGO or .ONG TLD, the name must comply with the validation requirements for eligibility to register names in that domain that are set forth in the operational standards, policies, procedures, and practices for the Registry TLD established from time to time by PIR pursuant to this Agreement.

Registrar will display the text of PIR's Registration Policies for .NGO and .ONG domain names (either through hyperlink to the Policies or displaying the text directly) and will implement measures to ensure that the registration cannot continue unless the prospective Registered Name Holder affirmatively indicates acceptance of all terms and conditions relating to the name.

Schedule C
Registration Fees

1. Payment of PIR Fees. In advance of incurring Fees, Registrar shall provide a payment security comprised of an irrevocable letter of credit, cash deposit, or other credit facility accepted by PIR ("**Payment Security**"), against which registration fees are charged at the time the domain name is registered. All Fees are due immediately upon receipt of applications for initial and renewal registrations, registrations associated with transfers of sponsorship, or upon provision of other services provided by PIR to Registrar. Payment shall be made via debit or draw down of the deposit account, irrevocable letter of credit or other credit facility, or payment method as deemed acceptable by PIR in its sole discretion. PIR shall provide monthly invoice statements to the Registrar.

2. Non-Payment of Fees. In the event Registrar has insufficient funds deposited or available through the irrevocable letter of credit or credit facility with PIR, PIR may do any or all of the following: (a) stop accepting new initial or renewal registrations, or registrations associated with transfers of sponsorship, from Registrar; (b) delete the domain names associated with any negative balance incurred or invoice not paid in full from the Registry database; (c) give written notice of termination of this Agreement; and (d) pursue any other available remedy under this Agreement or at law.

3. Domain Name Standard Initial Registration Fee. Other than Premium Domain Names (defined below), PIR will charge a standard fee per annual increment of an initial registration of a Registered Name (the "**Standard Initial Registration Fee**"). The Standard Initial Registration Fee shall be paid in full by Registrar sponsoring the domain name at the time of registration. PIR may increase the Standard Initial Registration Fee pursuant to Section 4 of the Agreement. The current Standard Initial Registration Fees are:

PIR TLD	STANDARD INITIAL REGISTRATION FEE (USD $)
.ORG	$9.93
.NGO	$15
.ONG	$15
.CHARITY	$21.50
.GIVES	$21.50
.GIVING	$21.50
.FOUNDATION	$21.50
.ОРГ (.xn--c1avg)	$8.25
.机构 (.xn--nqv7f)	$8.25
.संगठन (.xn--i1b6b1a6a2e)	$8.25

4. Domain Name Standard Renewal Fee. Other than Premium Domain Names, PIR will charge a standard fee per annual increment of a renewal of a Registered Name (the "**Standard Renewal Fee**") in the PIR TLDs. The Standard Renewal Fee shall be paid in full by Registrar sponsoring the domain name at the time of renewal. PIR may increase the Standard Renewal Fee pursuant to Section 4 of the Agreement. The current Standard Renewal Fees are:

PIR TLD	STANDARD RENEWAL FEE (USD $)
.ORG	$9.93
.NGO	$15
.ONG	$15
.CHARITY	$21.50
.GIVES	$21.50
.GIVING	$21.50
.FOUNDATION	$21.50
.ОРГ (.xn--c1avg)	$8.25
.机构 (.xn--nqv7f)	$8.25
.संगठन (.xn--i1b6b1a6a2e)	$8.25

5. Premium Domain Names and Pricing Tiers.

5.1. With the exception of .ORG, PIR may, at its sole discretion, establish a higher tiered-based pricing structure for both initial registration fees ("**Premium Initial Registration Fees**") and renewal fees for domains with Premium Initial Registration Fees ("**Premium Renewal Fees**") for certain second level domain names ("**Premium Domain Names**"). If any Premium Domain Names are designated or such pricing tiers are established, PIR shall publish the pricing in the Registrar Relations section of the PIR Website. For the PIR TLDs other than .ORG, PIR shall have the right, in its sole discretion, to modify Premium Domain Name tiers provided that gives no less than forty-five (45) days prior notice of any changes to tiers for Premium Initial Registration Fees, and no less than one hundred eighty (180) days' to modify the pricing of Premium Renewal Fee tiers. For the avoidance of doubt, PIR will not change the tier of a specific second level domain name for the entire duration of that registration.

5.2. For .ORG domain names, PIR may only charge premium pricing for the remaining reserved single and two character domain names pursuant to the Phased Allocation Program approved in the .ORG Registry Agreement.

6. Fees for Transfers of Sponsorship of Domain Name Registrations. Where the sponsorship of a Registered Name is transferred from one ICANN-Accredited Registrar to another ICANN-Accredited Registrar, PIR will require the registrar receiving the sponsorship to request a renewal of one year for the name. In connection with that extension, PIR will charge a renewal fee corresponding to the applicable (i) Standard Renewal Fee (the "**Standard Transfer Fee,**" the **Standard Transfer Fee**, the **Standard Initial Registration Fee,** and the **Standard Renewal Fee** are collectively, the "**Standard Fees**"); or (ii) the Premium Renewal Fee for the requested extension.

7. Bulk Transfers. For a bulk transfer approved by ICANN under Part B of the Transfer Policy, Registrar shall pay PIR US $0 (for transfer of 50,000 names or fewer) or US $50,000 (for transfers of more than 50,000 Registered Names).

8. Restore Fee. Registrar shall pay PIR a fee (the "**Restore Fee**") per Registered Name restored during the Redemption Grace Period though PIR reserves the right, in its sole discretion, to lower such fee based on extenuating circumstances. PIR shall have the right to raise the Restore Fee provided that it gives no less than one hundred eighty (180) days notice to Registrar. The current Restore Fees are:

PIR TLD	**RESTORE FEE (USD $)**
.ORG	$40
.NGO	$40
.ONG	$40
.CHARITY	$40
.GIVES	$40
.GIVING	$40
.FOUNDATION	$40
.ОРГ (.xn--c1avg)	$40
.机构 (.xn--nqv7f)	$40
.संगठन (.xn--i1b6b1a6a2e)	$40

9. Excess Deletion Fee. PIR may charge registrars a fee (the "**Excess Deletion Fee**") pursuant to ICANN's AGP (Add Grace Period) Limits Policy.

Exhibit 1

RRA Data Processing Addendum

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

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

1. INTRODUCTION

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

2. DEFINITIONS

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

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

c) Disclosing Party. Means the Party that transfers Shared Personal Data to the Receiving Party.

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

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

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

g) Personal Data. Means any information such as a name, an identification number, location

data, an online identifier or information pertaining to an individual's physical, physiological, genetic, mental, economic, cultural or social identity relating to that natural person, that can be used to directly or indirectly identify a Data Subject.

h) Processing. Means any operation or set of operations which is performed on the Shared Personal Data, whether or not by automated means, and which includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing, Processes, Processed or other derivatives as used herein, will have the same meaning.

i) Purpose(s). Has the meaning provided in Section 3 below.

j) Receiving Party. Means the Party receiving Shared Personal Data from the Disclosing Party.

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

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

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

3. PURPOSE, SUBJECT MATTER, AND ROLES

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

b) Subject Matter. This Data Processing Addendum sets out the framework for the protection of Shared Personal Data for the Purposes noted in this section and defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other. The Parties collectively acknowledge and agree that Processing necessitated by the Purpose(s) is to be performed at different stages, or at times even simultaneously by the Parties. Thus, this Data Processing Addendum is required to ensure that where Shared Personal Data may be Processed, it is done so at all times in compliance with the requirements of Applicable Laws.

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

i. The details of Processing are established and set forth in Annex 1;

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

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

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

4. FAIR AND LAWFUL PROCESSING

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

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

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

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

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

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

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

5. PROCESSING SHARED PERSONAL DATA

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

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

Those Standard Contractual Clauses (updated by 4 June 2021 EC decision: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-

transfers_en) are attached hereto and incorporated herein as Annex 2: Standard Contractual Clauses to Schedule B. For purposes of the RRA, the SCCs incorporate Module 1, Controller to Controller clauses. For the purposes of the RRA, the Registrar assumes and agrees to the obligations of the "Data Exporter" and Registry assumes and agrees to the obligations of the defined "Data Importer" in the Standard Contractual Clauses as if they had separately signed them in each instance for the respective Data Importer and Exporter.

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

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

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

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

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

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

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

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

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

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

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

h) Each Party will, at its expense, defend, indemnify and hold the other Party harmless from and against all claims, liabilities, costs and expenses arising from or relating to (i) a Data Security

Breach, (ii) breach of Applicable Laws, and (iii) breach of this Data Processing Addendum, to the extent the cause of the breaching Party's negligent, willful or intentional acts or omissions.

i) The Parties shall, in respect of Shared Personal Data, ensure that their privacy notices are clear and provide sufficient information to Data Subjects in order for them to understand what of their Personal Data is included in Shared Personal Data, the circumstances in which it will be shared, the purposes for the Personal Data sharing and either the identity with whom the Personal Data is shared or a description of the type of organization that will receive the Shared Personal Data.

j) The Parties undertake to inform Data Subjects of the Purposes for which it will process the Shared Personal Data and provide all of the information that it must provide in accordance with Applicable Laws, to ensure that the Data Subjects understand how their Personal Data will be Processed.

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

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

6. SECURITY

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

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

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

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

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

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

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

vi. Limiting access to relevant databases and systems to those of its officers, staff, agents, vendors and subcontractors who need to have access to the Shared Personal Data, and ensuring that password security mechanisms are in place to prevent inappropriate access when individuals are no longer engaged by the Party;

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

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

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

7. SECURITY BREACH NOTIFICATION

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

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

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

ii. Expected resolution time (if known);

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

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

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

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

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

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

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

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

8. DATA SUBJECT RIGHTS

a) Controllers have certain obligations to respond to requests of a Data Subject whose Personal Data is being processed under this Data Processing Addendum, and who wishes to exercise any of their rights under Applicable Laws, including, but not limited to: (i) right of access and update; (ii) right to data portability; (iii) right to erasure; (iv) right to rectification; (v) right to object to automated decision-making; or (vi) right to object to processing.

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

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

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

9. DATA RETENTION AND DELETION

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

10. TRANSFERS

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

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

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

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

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

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

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

11. RESOLUTION OF DISPUTES

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

b) The Parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by a Data Protection Authority. If they do participate in the proceedings, the Parties may elect to do so remotely (such as by telephone or other electronic means). The Parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

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

12. IMPACT OF CHANGES; NEW GUIDANCE

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

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

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

Annex 1

DETAILS OF THE PROCESSING

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

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

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

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

Annex II

EUROPEAN COMMISSION

Brussels, 4.6.2021
C(2021) 3972 final ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

EN

EN

ANNEX

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)[1] 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

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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 ~~– Optional~~

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.

MODULE ONE: Transfer controller to controller

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[2] 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.

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(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[3] (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.

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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.

~~**MODULE TWO: Transfer controller to processor**~~

~~**8.1 Instructions**~~

~~(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.~~

~~(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.~~

~~**8.2 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, unless on further instructions from the data exporter.~~

~~**8.3 Transparency**~~

~~On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.~~

~~**8.4 Accuracy**~~

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 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 data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties 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 subjects. 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. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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 breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach.

Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide allinformation at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 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 and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer 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 Regulation of (EU) 2016/679 with respect to the processing in question;

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[5].

[5] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

8.2 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., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter 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.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 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 data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (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. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive

control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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 breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 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 and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[6]

[6] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

(in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer 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;

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and 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 of the personal data[7], the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and 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 data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

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

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

[7] This includes whether the transfer and further processing 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.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub- processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[8] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub- processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub- processors at least [*Specify time period*] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[9] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the

~~sub-processor contract and to instruct the sub-processor to erase or return the personal data.~~

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

(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.[10] 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:

[10] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(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.

~~**MODULE TWO: Transfer controller to processor**~~

~~(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.~~

~~(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.~~

~~(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.~~

~~**MODULE THREE: Transfer processor to processor**~~

~~(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.~~

~~(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.~~

~~(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.~~

~~**MODULE FOUR: Transfer processor to controller**~~

~~The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.~~

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[11] 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.]~~

MODULE ONE: Transfer controller to controller

~~**MODULE TWO: Transfer controller to processor**~~

~~**MODULE THREE: Transfer processor to processor**~~

(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.

[11] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(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

MODULE ONE: Transfer controller to controller

~~**MODULE FOUR: Transfer processor to controller**~~

(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.

~~**MODULE TWO: Transfer controller to processor**~~

~~**MODULE THREE: Transfer processor to processor**~~

~~(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) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.~~

~~(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.~~

~~(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.~~

~~(e) 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.~~

~~(f) The Parties agree that if one Party is held liable under paragraph (e), 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.~~

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

Clause 13

Supervision

MODULE ONE: Transfer controller to controller

~~**MODULE TWO: Transfer controller to processor**~~

~~**MODULE THREE: Transfer processor to processor**~~

~~(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

MODULE ONE: Transfer controller to controller

~~**MODULE TWO: Transfer controller to processor**~~

~~**MODULE THREE: Transfer processor to processor**~~

~~**MODULE FOUR: Transfer processor to controller** *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*~~

(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[12];

[12] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(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). ~~[For Module Three: The data exporter shall forward the notification to the controller.]~~

(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 ~~[for Module Three: , if appropriate in consultation with the controller]~~. 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 ~~[for Module Three: the controller or]~~ 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

MODULE ONE: Transfer controller to controller

~~**MODULE TWO: Transfer controller to processor**~~

~~**MODULE THREE: Transfer processor to processor**~~

~~**MODULE FOUR: Transfer processor to controller** *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*~~

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.

~~[For Module Three: The data exporter shall forward the notification to the controller.]~~

(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.). ~~[For Module Three: The data exporter shall forward the information to the controller.]~~

(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

(a) 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).

(b) 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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) 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 [for Module Three: and the controller] 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) [For Modules One, Two and Three: 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.] ~~[For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.]~~ 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

MODULE ONE: Transfer controller to controller

~~**MODULE TWO: Transfer controller to processor**~~

~~**MODULE THREE: Transfer processor to processor**~~

[OPTION 1: 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 Germany (*specify Member State*).]

~~[OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of ___ (*specify Member State*).]~~

~~**MODULE FOUR: Transfer processor to controller**~~

~~These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify country*).~~

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller ~~**MODULE TWO: Transfer controller to processor**~~ ~~**MODULE THREE: Transfer processor to processor**~~

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

(b) The Parties agree that those shall be the courts of Germany (*specify Member State*). 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.

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

~~**MODULE FOUR: Transfer processor to controller**~~

~~Any dispute arising from these Clauses shall be resolved by the courts of _____ (*specify country*).~~

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 be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

~~**MODULE TWO: Transfer controller to processor**~~

~~**MODULE THREE: Transfer processor to processor**~~

~~**MODULE FOUR: Transfer processor to controller**~~

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]*

1. Name: … Address: …
Contact person's name, position and contact details: … Activities relevant to the data transferred under these Clauses: See Section 3(a) of the Data Processing Addendum
Signature and date: …
Role(controller/processor):Controller

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

1. Name:Public Interest Registry

Address:11911 Freedom Drive

10th Floor, Suite 1000

Reston, VA 20190
Contact person's name, position and contact details: privacy@pir.org
Activities relevant to the data transferred under these Clauses:See Section 3(a) of the Data Processing Addendum
Signature and date: …
Role (controller/processor): Controller

2. …

B. DESCRIPTION OF TRANSFER MODULE

ONE: Transfer controller to controller ~~MODULE~~

~~TWO: Transfer controller to processor MODULE~~

~~THREE: Transfer processor to processor MODULE~~

~~FOUR: Transfer processor to controller~~

Categories of data subjects whose personal data is transferred

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

Categories of personal data transferred

Natural person's data can include registrant's information provided to registrars upon registration of a domain name (registrant name, address, email, phone number, IP address) commonly known as "WHOIS" data (see also Annex 1 of the Data Processing Addendum).

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. Not Applicable

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

Nature of the processing

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

Purpose(s) of the data transfer and further processing

See DPA Section 3(a) for purposes of processing and further processing.

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

Data is retained for the life of the registration plus a minimum of 2 years (this is subject to change per requirements via ICANN Consensus Policies.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Any transfer to sub-processors would be to fulfill the promised services. It may be occasional or continuous depending upon the sub-processor.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

~~**MODULE TWO: Transfer controller to processor**~~

~~**MODULE THREE: Transfer processor to processor**~~

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

State Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia

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

MODULE ONE: Transfer controller to controller ~~**MODULE TWO: Transfer controller to processor**~~ ~~**MODULE THREE: Transfer processor to processor**~~

Security Measures

Controller aims to comply with relevant industry standard security measures as well as with all applicable data privacy and security laws, regulations and standards.

Controller is continuously evaluating its security measures and improving its position as these standards and regulations evolve as well as to respond to new security risks.

Technical Measures

Cloud based SaaS offering are utilized for data storage and visualization.

- These systems have SOC 2 Compliance covering security, availability, processing integrity, confidentiality and privacy measures.

Organizational Measures

- Governance and authorization process to ensure all PII data is used in accordance with legal bases.
- Controller maintains a dedicated Data Governance lead that oversees how data is collected, its uses, its access, and its retention.
- All data has a designated Data Owner, charged with classifying data and determining appropriate access levels.
- All data has a designated Data Steward, charged with defining data quality standards and data certification.
- Users are trained on appropriate use of data and PII.
- Users are authenticated via enterprise SSO and multi-factor authorization is enabled.
- Controller maintains processes and procedures to ensure that all development is performed in a secure manner and following a standard development lifecycle process.
- Controller maintains processes and procedures to define requirements around enforcing security and access measures as they relate to employment status changes.
- Controller maintains procedures around data classification, data encryption, and rules for transmission.
- Controller maintains procedures around business continuity and disaster recovery.
- Controller's security team can be reached at privacy@pir.org for issues or question.