

THIS AGREEMENT HAS A PROVISION FOR ARBITRATION OF DISPUTES BETWEEN THE PARTIES.

This Reseller Agreement ("RSA") is a legal agreement by and between you, as you have identified yourself in your account information ("You" and "Your"), the backend service provider, eNom, Incorporated. ("eNom") and, the primary service provider, {{orgName}} (the "Primary Service Provider"). If You are buying the Services (defined below) directly from eNom, eNom is both Your backend service provider and your Primary Service Provider. You warrant that the information You provide in Your account with eNom ("Your Account") is accurate and that You will keep it updated. This RSA sets forth the terms and conditions of Your use and resale of eNom's Domain Name Registration and related services ("Services"). By using the Services, You acknowledge that You have read, understand and agree to be bound by this RSA, along with any additional terms, conditions or policies which eNom or ICANN may establish from time to time, the current version of which can be found here <http://www.enom.com/terms/default.asp>. In addition to transactions entered into by You on Your behalf, You also agree to be bound by this RSA for transactions entered into on Your behalf by anyone acting as Your agent, and transactions entered into by anyone who uses Your Account. This RSA will only be effective upon eNom's provision of the Services to You. The terms and conditions of this RSA may be modified from time to time by eNom. Such modifications become effective 30 days after eNom notifies You of the modifications or immediately upon Your express consent to the revised terms and are effective from that date forward. You agree that we may notify You of the modifications by, for example, sending email to You at Your email address of record. If You do not agree to the terms and conditions of this RSA as modified, You may send us a cancellation notice and You will remain subject to the unmodified terms and conditions of this RSA (except Section 5 ICANN Obligations will apply to You) for the remainder of the term of the RSA, after which Your RSA will terminate.

1. Reselling the Services.

- A. Subject to the terms and conditions of this RSA, eNom grants You a non-exclusive, non-transferable license to resell the Services worldwide. The Services include, but are not limited to those Services listed on our site at <http://www.enom.com/reseller/default.asp> and any other Services as eNom may make available in Your Account from time to time. Certain of the Services are offered only subject to additional terms and conditions which are available at <http://www.enom.com/terms/> (e.g., the eNom Registration Agreement at <http://www.enom.com/terms/agreement.aspx>, the ID Protect Agreement at <http://www.enom.com/terms/idprotect-agreement.aspx>, etc.). To resell

these Services, You and Your Sub-Resellers (defined below) and each of Your end customers purchasing these Services must agree to these additional terms and conditions as they may be updated from time to time. You agree to indemnify and hold harmless eNom for any failure by You or a Sub-Reseller below Your Account to obtain the consent of any Sub-Reseller or customer to these additional terms and conditions. The Services do not include other services which are not made available through Your Account by eNom, its third-party licensors or a Primary Service Provider other than eNom. If Your Primary Service Provider is not eNom, it is an independent reseller of eNom and may offer its own services under separate agreement.

- B. You may authorize sub-resellers on Your Account to resell the Services ("Sub-Resellers") via accounts attached to Your Account ("Sub-Accounts"). You are responsible to eNom for the costs, fees, expenses, acts and omissions of Your Sub-Resellers and any Sub-Resellers "below" them in Your Account or any Sub-Accounts. You are required to have all Sub-Resellers acknowledge and agree to the terms of this RSA. You agree to comply and ensure compliance by Your Sub-Resellers with this RSA, all applicable eNom or ICANN policies, laws and regulations in reselling the Services. In the event a Sub-Reseller's Sub-Account is terminated by the Sub-Reseller, You or eNom, You will be responsible for the Sub-Account.
- C. If You stop using Your Account, become unavailable to eNom, Your Primary Service Provider (if applicable), Your customers or Sub-Resellers, or this RSA is terminated by eNom for any reason, eNom may, but is not obligated to, assume direct control over any of Your customers and/or Sub-Accounts.

2. Points, payments, and commissions.

- A. You may be required to purchase "Points" to obtain all or certain of the Services. When You purchase Points, Your price for the Points may also include certain costs, such as online taxes and a convenience fee established by eNom (currently set at 5%, subject to change at any time in eNom's sole discretion), which will not be reflected in Your Point total. For example, when You pay \$100 toward the purchase of Points with Your credit card or PayPal account, You will be charged a convenience fee for online access, and in the event the convenience fee is 5%, and 95 Points will be deposited into Your Account. You agree to pay, prior to the effectiveness of the desired Services, the applicable

Service fees communicated to You. If You have a Primary Service Provider other than eNom, Your pricing for the Services is determined by Your Primary Service Provider. eNom accepts checks and/or wire transfers with no additional charges. Please contact eNom to arrange such a payment. Points are non-refundable for any reason and are not transferable without the consent of eNom, which may be denied for any reason. You will be responsible for all merchant services fees, outlined in the Merchant Services Agreement at http://www.enom.com/terms/terms_ccAgreement.asp for any transaction originating from all Sub-Accounts below Your Account.

- B. Points and certain of the Services may be purchased using a credit card. You authorize eNom to debit the credit card You present in relation to a particular transaction or the credit card You otherwise provide through Your Account. You must present only approved transactions to eNom. Prior to contacting Your credit card company in relation to such charges, You will first contact Your Primary Service Provider (if Your Primary Service Provider is not eNom) and thereafter eNom to verify the charges and the manner of billing. You must require all Sub-Resellers and all customers in and below Your Account to only present approved transactions to eNom and to contact eNom regarding charges, as described above. Any chargeback by a credit card company or similar action by or through another payment provider relating to payment to eNom, for whatever reason, whether by You, by any Sub-Reseller or customer below Your Account i) is a material breach of this RSA, ii) is an act for which You agree to be jointly and severally liable to make eNom whole, iii) is an act with respect to which eNom will charge \$35.00 per incident, in addition to merchant services fees and other payment provider service charges which may be charged to eNom, and iv) that the same shall be grounds for suspension and/or termination of this RSA and the Services. Under such circumstances, eNom may suspend Your access to any and all of Your Accounts and may assume all right, title, interest in, and use of any domain name registration(s) and/or websites, email, or other data hosted on systems controlled by eNom (the "Collateral"). eNom will reinstate rights in the Collateral solely in its discretion, subject to receipt of the fee(s) owed and the then-current reinstatement fee, currently set at US\$200. You hereby acknowledge and consent to eNom's right, but not obligation, to sell, dispose of, or retain the Collateral if eNom determines the same to be a means of obtaining some monetary or other satisfaction or security, even

if You assert that the value of the Collateral exceeds the amount You owe eNom.

- C. eNom may require that You pay for Points or the Services using a particular payment means, such as by wire transfer. eNom may also demand reasonable assurance of payment at eNom's sole discretion.
- D. If You are using eNom's merchant services provider (credit card processing company), receipts from Your customers and Sub-Resellers will be processed by the merchant services provider(s) selected by eNom and will be subject to convenience fees, taxes any and ICANN fees or assessments.
- E. You authorize eNom to deduct from Your Points any amounts owed by You to eNom, including, without limitation, amounts owed as a result of Your indemnification of eNom for third party claims and any administrative costs, including reasonable administrative costs which may be charged for inactive accounts.
- F. You authorize eNom to sell, take title to, and/or use any Collateral as a means of obtaining some monetary or other satisfaction for any amounts owed by You to eNom, including, without limitation, amounts owed as a result of Your indemnification of eNom for third party claims and any administrative costs, including reasonable administrative costs which may be charged for inactive accounts.
- G. If You have Sub-Account(s) below Your Account, You may earn commissions from sales generated by such Sub-Account(s). Such commissions will amount to the difference between the following: i) the price You charge the Sub-Reseller, less merchant service fees, taxes and ICANN fees; and ii) the price You are charged for the Services. When You have a balance greater than \$25.00 (U.S.) in commissions which have aged more than 90 days (which allows time for chargebacks and reversed transactions), You will be able to have Your commissions transferred to Your Account balance, sent to You via a check deposited in the U.S. mail (another reason to keep Your Account information current) or via direct deposit, when and if direct deposit becomes available. Commissions will be reported through Your Account in Your Available Commission Balance. Your Point balance is not part of Your Available Commission Balance.

3. **Support.** You are responsible for providing customer service, billing, and technical support to Your customers, Sub-Resellers and customers of Your Sub-Resellers. eNom will provide telephone and/or email support to You 24 hours, 7 days per week. eNom may, but is not obligated to, provide support directly to Your customers. If eNom receives communications from registrants or from third-parties regarding Services provided in Your Account or any Sub-Accounts, eNom will, where appropriate, forward such communications to You, the applicable Sub-Reseller, or the Primary Service Provider (if Your Primary Service Provider is not eNom) at eNom's discretion for further action; however, reserves the right to respond to such communications directly. If eNom determines that You are providing inadequate support to Your customers or Sub-Resellers (resulting in, for example, an excessive number of support calls directly from Your customers), You will be in breach of this RSA and eNom may terminate this RSA.

4. **4. Licensed Use of Trademarks and Technology.** The Services may only be accessed through the application programming interface (including the associated documentation, the "API"), Your Account, websites created by eNom which use the API, updates and upgrades thereto, and through such other means and technologies which eNom makes available through its websites or downloads (collectively, the "Technology").
 - A. eNom hereby grants to You a non-exclusive, non-transferable, royalty-free, terminable license, exercisable solely during the term of this RSA, to use the Technology solely for the purpose of accessing and using the Services. With the exception of Your Account, this license right may be sublicensed to Sub-Resellers in Your Account and in Sub-Accounts below Your Account, but only subject to all license terms and restrictions of this RSA, only during the term of this RSA, and only so long as performance of the Services by eNom has not been suspended.

 - B. eNom hereby grants You a non-exclusive, worldwide, fully paid up, royalty free, terminable right and license to use eNom's trademarks (the "Trademarks") solely as provided by eNom and solely as pre-approved in writing in connection with the marketing and promotion of the Services. All approved uses of Trademarks will inure to the benefit of eNom and must comply with eNom's Trademark and Branding Guidelines at http://www.enom.com/terms/branding_guideline.asp.

 - C. Except for the rights expressly granted above, this RSA does not transfer from eNom to You or Your customers any eNom Trademarks, technology or intellectual property rights, and all rights, titles and

interests in and to the Trademarks, Technology and intellectual property remain solely with eNom.

- D. You shall not, directly or indirectly, reverse engineer, decompile, disassemble or otherwise attempt to derive source code or other trade secrets from the Technology.
 - E. You shall not branch or otherwise prepare derivatives of the API.
 - F. You shall not copy or use the Technology except as specified in this RSA.
 - G. You shall not create, apply for, or otherwise procure any rights in any Trademarks or any patent or copyright interest in the Technology and any derivative thereof ("IP Interest") which IP Interest would block, impede, or make more expensive eNom's continued use and enjoyment of the Technology. If You breach the provisions of this Section, any IP Interests created thereby shall be assigned to eNom at the point they are fixed in tangible form. You agree to execute any documents necessary to affect an assignment of any such IP Interests to eNom without compensation.
 - H. You shall not use the Technology to communicate with or control a system other than one(s) designated by eNom, and You may not access the Services using any access mechanism other than the Technology.
 - I. You shall not abuse the Service infrastructure. "Abuse" in the foregoing sentence means, by way of example and without limitation, any action or conduct which degrades service to other users of the shared Services and Technology.
5. **ICANN Obligations.** Pursuant to eNom's Registrar Accreditation Agreement with ICANN (a current version of which can be found [here](#)) (the "RAA") You must comply with the following terms:
- A. You must not display the ICANN or ICANN-Accredited Registrar logo, or otherwise represent Yourself as accredited by ICANN unless You have written permission from ICANN to do so.
 - B. For the avoidance of doubt. You shall require all of Your Customers and Sub-Resellers to enter into an electronic or paper registration agreement (<http://www.enom.com/terms/agreement.aspx>). Without limiting the

generality of anything herein, the registration agreement You use with Your customers and Sub-Resellers shall (i) include all registration agreement provisions and notices required by the RAA and any [ICANN Consensus Policies](#), (ii) identify eNom as the sponsoring registrar or provide a means for identifying the sponsoring registrar, such as a link to the InterNIC Whois lookup service; and (iii) explicitly authorize eNom to act as the registrant's "Designated Agent" (as defined in ICANN's transfer policy) to approve each "Change in Registrant" (as defined in ICANN's transfer policy) on the registrant's behalf. Notwithstanding the foregoing You shall modify all "Pricing Page" hyperlinks in the eNom Registration Agreement (<http://www.enom.com/terms/agreement.aspx>) to point to a pricing page on your website which publishes Your domain name registration fees, renewal fees, transfer fees, post-expiration renewal fees (if different) and redemption/restore fees. In addition, You must identify eNom as the sponsoring registrar upon inquiry from Your customer or Sub-Resellers.

- C. You must comply with any ICANN-adopted specification or policy that establishes a program for accreditation of individuals or entities who provide proxy and privacy registration services (a "Proxy Accreditation Program"). Among other features, the Proxy Accreditation Program may require that proxy and privacy registration services may only be provided in respect of domain name registrations by individuals or entities accredited by ICANN pursuant to such Proxy Accreditation Program. In such a case, You must not knowingly accept registrations from any provider of proxy and privacy registration services that is not Accredited by ICANN pursuant to the Proxy Accreditation Program. Until such time as the Proxy Accreditation Program is established, You must comply with the [Specification on Privacy and Proxy Registrations](#)
- D. ICANN has published an educational webpage summarizing the terms of the RAA and related consensus policies. You must provide a link to such webpage on any website You may operate for domain name registration or renewal, such link which must be clearly displayed to Your customers at least as clearly as You link to policies or notifications required to be displayed under ICANN consensus policies.
- E. You must publish on Your website(s) and/or provide a link to the [Registrants' Benefits and Responsibilities](#) and shall not take any action inconsistent with the RAA or applicable law.

- F. Any other terms and conditions which come into effect through the revision of the RAA by ICANN or through the introduction of any amended or new ICANN consensus policy, whether or not eNom gives You notice of such revisions, amendments, or new policies.

In addition to any other right to terminate set forth in this RSA, eNom specifically has the right to immediately terminate this RSA, without notice or right to cure, in the event that You violate any terms found in this Section 5.

- 6. **License by You to eNom.** In connection with providing materials to eNom in performance of the Services, You grant eNom a limited license to modify, adapt, incorporate with other material, and otherwise to use the materials provided by You but only to the extent necessary or useful to provide the Services as directed by You. You warrant that the materials provided by You to eNom are Your sole property or that You have obtained appropriate licenses to the material such that eNom's use of the material in providing the Services shall not subject eNom to a claim.
- 7. **Restrictions on Use of Services.** You must not make any representations or warranties about the Services to any of Your customers or Sub-Resellers or any other third party that are inconsistent with this RSA. You agree not to use the Services, or to allow Your customers or Sub-Resellers to use the Services for:
 - A. The transmission of unsolicited email (spam);
 - B. Repetitive, high volume inquires or other excessive use or abuse of the Services or Technology;
 - C. Any activity which results in eNom's IP addresses being reported to spam blocking organizations or other organizations which attempt to police or monitor abuse of the Internet;
 - D. Any illegal, dishonest, deceptive or unfair trade practices;
 - E. Any use which fails to abide by customary industry acceptable use policies or any applicable laws.

In addition to any other right to terminate set forth in this RSA, eNom specifically has the right to immediately terminate this RSA, without notice or right to cure, in the event that You violate any terms found in this Section 7.

8. **Suspension or Termination of the Services.** In addition to any other rights or remedies of eNom herein, eNom reserves the right to suspend performance of the Services or to preclude use of or access to the Technology in the event of an unresolved breach of this RSA or suspension or cancellation is required by any policy now in effect or later adopted by ICANN. You agree that Your failure to comply completely with the terms and conditions of this RSA and any eNom rule or policy may be considered to be a material breach of this RSA and eNom may provide You with notice of such breach either in writing or electronically (i.e. email). In the event You do not provide eNom with material evidence that You have not breached Your obligations within ten (10) business days, eNom may terminate this RSA and take any remedial action available to eNom under the applicable laws. Such remedial action may be implemented without notice to You and may include, but is not limited to, cancelling the registration of any of Your domain names and discontinuing any Services provided to You. No fees will be refunded to You should Your RSA be cancelled or Services be discontinued because of a breach.
9. **Term of this RSA and Termination.** This RSA is effective for a period of one year from the date of creation of Your Account by eNom. This RSA will then renew for an indefinite number of one-year terms. Upon at least thirty (30) days written notice (including notice via email), either party may terminate this RSA. eNom also retains the right to terminate this RSA immediately if eNom determines, in its sole discretion, that You, Your customers or Your Sub-Resellers have failed to comply with any term or condition of this RSA, or that Your use of the Services presents an unreasonable risk of harm to eNom or its affiliates, the Service, other users, or members of the general public.
10. **Confidentiality.** During the term of this RSA and for one (1) year thereafter, each party must treat the other party's Confidential Information as confidential, and must not use such Confidential Information except as expressly permitted under this RSA. Each party shall take reasonable measures to prevent the disclosure and unauthorized use of the Confidential Information of the other party; which shall be no less than the same degree of care that such party uses to protect its own like information. Neither party will use the other's Confidential Information for purposes other than those necessary to directly further the purposes of this RSA. Neither party will disclose to third parties the other's Confidential Information without the prior written consent of the other party. For purposes of this RSA "Confidential Information" means any non-public information relating to either party's business, product plans, designs, costs, prices and names, finances, business opportunities, personnel, research development or know-how. "Confidential Information" does not include information that: (i) is or becomes publicly known or available through no fault

of the receiving party; (ii) is already known by the receiving party at the time of disclosure; (iii) is independently developed or learned by the receiving party without reference to the other party's Confidential Information; or (iv) is lawfully obtained from a third party that does not have an obligation of confidentiality to the disclosing party. It is not a breach of this RSA to disclose Confidential Information of the other party pursuant to an order or requirement of a court, administrative agency, other governmental body, or securities exchange.

11. Disclaimer of Warranties. ENOM DOES NOT WARRANT THAT PERFORMANCE OF THE SERVICES OR USE OF THE TECHNOLOGY WILL BE UNINTERRUPTED, ERROR FREE, OR THAT IT WILL NOT BE NECESSARY FOR YOU TO PROVIDE NOTICE OF ERRORS TO YOUR CUSTOMERS OR SUB-RESELLERS.

12. Indemnification. You, at Your own expense, will indemnify, defend and hold harmless eNom and its employees, directors, officers, representatives, agents and affiliates against any claim, suit, action, or other proceeding based on or arising from any claim or alleged claim (i) arising from a breach by You of any covenant, representation or warranty in this RSA, including but not limited to the ICANN Obligations set forth in Section 5; (ii) relating to any product or service of Yours; (iii) relating to Your use or Your Sub-Resellers use of the Services; or (iv) relating to Your domain name registration and related service business, including, but not limited to, Your advertising, domain name application process, systems and other processes, fees charged, billing practices and customer service; provided, however, that in any such case: (a) eNom provides You with prompt notice of any such claim, and (b) upon Your written request, eNom provides You with all available information and assistance reasonably necessary for You to defend such claim, provided that You reimburse eNom for actual and reasonable costs. You shall not enter into any settlement or compromise of any such indemnifiable claim without eNom's prior written consent, which consent shall not be unreasonably withheld. You shall pay any and all costs, damages, and expenses, including, but not limited to, reasonable attorneys' fees and costs awarded against or otherwise incurred by eNom in connection with or arising from any such indemnifiable claim, suit, action or proceeding.

13. Limitation of Liability.

A. A material provision of entering into this RSA is that eNom's liability shall be limited as follows: In relation to each component of the Services for which a separate fee is charged, eNom shall be liable in an amount

no greater than the fees received by eNom for performing the specific transaction(s) that gave rise to the liability. eNom's aggregate liability for all claims of any sort shall not exceed the aggregate amount received by eNom from You over the term of this RSA. eNom shall not be liable for any unauthorized access to, or any corruption, erasure, theft, destruction, alteration, or inadvertent disclosure of data, information, or content transmitted, received, or stored on its or any third party systems. With respect to passwords, account identifiers, and other systems used to control access to Your Account, it is Your responsibility to safeguard such passwords, account identifiers, and other systems used to control access to Your Account. As a service to You, eNom may, but is not required to, take reasonable measures to verify the identity of parties who claim to have lost or forgotten passwords and/or account information and to then provide the information to such parties and that eNom shall not be responsible to You for losses or claims for any inadvertent disclosure of such passwords which may result thereby. eNom is entitled to email passwords to designated email account(s), to phone designated phone numbers, or to employ security questions as a means to verify the identity of the party entitled to control Your account.

B. EXCEPT AS EXPRESSLY PROVIDED IN THIS RSA, NEITHER PARTY SHALL BE LIABLE IN ANY WAY TO THE OTHER PARTY OR ANY OTHER PERSON FOR ANY LOST PROFITS OR REVENUES, LOSS OF USE, LOSS OF DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS, LICENSES, OR SERVICES OR SIMILAR ECONOMIC LOSS, OR FOR ANY PUNITIVE, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR SIMILAR DAMAGES OF ANY NATURE, WHETHER FORESEEABLE OR NOT, UNDER ANY WARRANTY OR OTHER RIGHT HEREUNDER, ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OR NON-PERFORMANCE OF THIS RSA, OR FOR ANY CLAIM AGAINST THE OTHER PARTY BY A THIRD PARTY, REGARDLESS OF WHETHER IT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH CLAIM OR DAMAGES.

14. Independent Contractors. The parties to this RSA are independent contractors and have no right or authority to bind or commit the other party in any way without the other party's express written authorization to do so. This RSA does not create an employer/employee, joint venture, partnership, or agency relationship between the parties.

15. **Audit.** During the term of this RSA and for seven (7) years thereafter, You must maintain (a) in electronic, paper, or microfilm form, all written communications constituting registration applications, confirmations, modifications, or terminations and related correspondence with Your customers, including registration contracts; and (b) in electronic form, records of the accounts of all Your customers, including dates and amounts of all payments and refunds in conjunction with domain name registrations. Upon request, You will provide any information identified in this Section 15 to eNom within two (2) business days and otherwise cooperate with eNom in any compliance, regulatory or legal issue arising out of the registration of domain names. Your failure to provide any such information to eNom within two (2) business days or Your failure to provide such cooperation will be a material breach of this RSA.
16. **Assignment.** You must not assign, transfer, or otherwise dispose of this RSA or any of Your rights, benefits, or interests under this RSA without prior written consent of eNom, and any such assignment in violation shall be void. eNom may also assign this RSA to a party which acquires the assets of eNom which relate to performance of this RSA. eNom may assign all or part of its rights and obligations under this RSA to its parent corporation, to a subsidiary, to its survivor in connection with a corporate reorganization, to any entity acquiring all or substantially all of its property, or to any entity into which it is merged or consolidated. No assignment of this RSA shall operate to discharge the assignor of any duty or obligations hereunder without prior written consent.
17. **Taxes.** Unless specified otherwise, the fees for the Service do not include taxes. If eNom is required to pay ICANN fees or United States or international sales, use, property, value-added, royalty, license or other taxes based on the licenses granted in this RSA or on Your use of the Services, then You must pay such taxes or fees. This section does not apply to taxes based on eNom's income.
18. **Force Majeure.** Neither party shall be in default or liable for any loss or damage resulting from delays in performance or from failure to perform or comply with terms of this RSA (other than the obligation to make payments, which shall not be affected by this provision) due to any causes beyond its reasonable control, which causes include but are not limited to Acts of God or the public enemy; riots and insurrections; war; fire; strikes and other labor difficulties (whether or not the party is in a position to concede to such demands); embargoes; judicial action; lack of or inability to obtain export permits or approvals, necessary labor, materials, energy, components or machinery; acts of civil or military authorities; failure of telecommunications; or other casualty.

19. Governing Law and Arbitration. This RSA shall be governed by the laws of the United States of America and the State of Washington, as if this RSA was a contract wholly entered into and wholly performed within the State of Washington. Any dispute, claim or controversy arising out of or relating to this RSA or the breach, termination, enforcement, interpretation or validity thereof, including the determination of the scope or applicability of the agreement to arbitrate, shall be determined by arbitration in King County, Washington, before one arbitrator. The arbitration shall be administered by JAMS pursuant to its Comprehensive Arbitration Rules and Procedures. Judgment on the Award may be entered in any court having jurisdiction. YOU AND ENOM AGREE THAT EACH MAY BRING CLAIMS AGAINST THE OTHER ONLY IN AN INDIVIDUAL CAPACITY, AND NOT AS A CLASS MEMBER IN ANY FORM OF A CLASS PROCEEDING. Further, unless both You and eNom expressly agree otherwise in writing, the arbitrator may not consolidate more than one person's claims and may not otherwise preside over any form of a class proceeding. This clause shall not preclude parties from seeking provisional remedies in aid of arbitration from a court of appropriate jurisdiction.

20. Applicable Laws. You represent and warrant that You will comply with all applicable laws and regulations. Without limiting the generality of the foregoing, You represent and warrant that: (i) You will not act in any fashion or take any action that will render the Backend Service Provider or Primary Service Provider liable for a violation of any applicable anti-bribery regulation (including without limitation, the U.S. Foreign Corrupt Practices Act and the UK Bribery Act 2010); and (ii) You will comply with U.S. laws that prohibit or limit the ability of U.S. persons from directly or indirectly exporting or providing goods or services to certain persons or countries. You shall comply with all U.S. export regulations if shipping to another country, including licensing requirements.

21. Privacy Laws. As used in this Agreement, "Personal Data" means any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. If You collect Personal Data related to the services provided under this RSA, you will provide a clear and conspicuous privacy notice to such individuals that accurately describes to such Data Subjects what you collect and process, in compliance with applicable laws.

In the event Customer decides to offer any domain name or other service under this Agreement that requires the collection, processing or transfer of Personal Data that is subject to law or regulation concerning data protection and information security that governs the processing of Personal Data including the European Union's Regulation 2016/679 Data Protection Laws, the Parties will comply with the additional obligations and warranties set out in the Data Processing Addendum incorporated into this Agreement as Appendix A. If, at any time, the Data Protection Laws require any further steps to be taken in order to permit the collection, processing or transfer Personal Data as envisaged under this Agreement, then You will take all steps reasonably required by Enom (including, when necessary, entering into contractual clauses with Enom) to ensure that the transfer of the Personal Data meets the requirements of Data Protection Laws.

22. **Security Requirements.** If you employ any third-party providers to support your provisioning of services under this RSA, you will contractually require such providers to protect the privacy, confidentiality, and security of Data Subjects using at least the same level of protection that applies to You under this RSA.
23. **Additional Registry Requirements.** Some [registries](#) have additional contractual requirements that you agree to by reselling domain name registration services or other services for those [registries](#). You are responsible for reviewing any terms and conditions applicable to or provided by such [registries](#). In addition, without limiting the generality of anything herein, the registration agreement You use with Your customers and Sub-Resellers shall include all terms and conditions required by the [registries](#) which you resell domain name registration services or other services for. Such terms and conditions linked in the eNom Registration Agreement. More information about these additional contractual terms can be found on our website at: <https://www.enom.com/terms/terms-reseller-additional.aspx>
24. **General.** The parties hereby incorporate the requirements of 41 CFR 60-1.4(a), 300.5(a) and 741.5, if applicable. This RSA, together with all modifications, constitute the complete and exclusive agreement between You and eNom, and supersedes and governs all prior proposals, agreements, or other communications and is not intended to confer upon any person or entity other than eNom and You any rights or remedies hereunder. You represent, warrant, and agree that upon entering into this RSA, that You are not relying upon and have not relied upon any representation, promise, or statement made by anyone which is not recited, contained, or embodied in this RSA. The failure of us to require Your performance of any provision hereof shall not affect the full right to require such performance at any time thereafter; nor shall the waiver by us of

a breach of any provision hereof be taken or held to be a waiver of the provision itself. In the event that any provision of this RSA shall be unenforceable or invalid under any applicable law or be so held by applicable court decision, such unenforceability or invalidity shall not render this RSA unenforceable or invalid as a whole. We will amend or replace such provision with one that is valid and enforceable and which achieves, to the extent possible, our original objectives and intent as reflected in the original provision.

Appendix A

Data Processing Addendum (Revision May 2018)

Agreement entered into by and between
Customer, as identified in Enom Master Services Agreement
– “Controller” or “Joint Controller” or “Customer” –

and

Enom, LLC
5808 Lake Washington Blvd. NE, Suite 201
Kirkland, WA 98033, USA
– “Processor” or “Joint Controller” or “Enom” –

Preamble

This Data Processing Agreement (“DPA”) defines and sets out in detail the data protection obligations of the contracting parties arising under the Reseller Agreement (“RSA”) entered by the parties. It applies to all activities relating to the RSA where employees of the Processor or other persons or parties engaged by the Processor may encounter personal data of the Controller and when the parties may act as Joint Controllers.

For the purposes of this DPA, the following terms have the following meaning:

(a) “Data Protection Authority” means an administrative, supervisory, or law enforcement authority or other governmental body with responsibility for the enforcement of Data Protection Laws.

(b) “Data Protection Laws” means any applicable law or regulation concerning data protection and information security that governs the processing of Personal Data under this Agreement, including the European Union’s Regulation 2016/679 (“General Data Protection Regulation” or “GDPR”).

(c) “Personal Data” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

(d) “Processing”, “Processed” or “Process”, when capitalized herein, means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

* * *

1. Subject matter, term and specification of the Data Processing

- 1.1. The RSA specifies the subject matter and the term of the agreed contract data processing as well as the scope and nature of data collection, data processing and use of data. The specific data being processed is outlined in Enom’ Data Use Information Page. The term and termination of this agreement follows the term and termination agreed upon in the RSA. Termination of the RSA will automatically result in the termination of this DPA.
- 1.2. The Processor’s registered office is located in Canada, which is a country with laws that do not ensure an adequate level of data protection according to European Union’s “General Data Protection Regulation” (GDPR) requirements. Any transfer of personal data in context of this agreement is governed by the standard contractual clauses in **Annex A**.

2. Scope of Application and Responsibility

- 2.1.** The Processor processes personal data on behalf of the Controller, and at the direction of ICANN and third-party registries. This includes all activities specified in the RSA. The Controller is responsible under this agreement for compliance with the statutory provisions in the data protection and data privacy laws applicable in its registered place of business, including, but not limited to, ensuring that any disclosure, or passing of data, to the Processor as well as any data processing is lawful.
- 2.2.** Data processing requirements and instructions are stipulated in the RSA and may subsequently be changed, modified, amended, or replaced in writing.
- 2.3.** If the Processor determines that a permissible individual instruction is contrary to the applicable data protection or privacy law, it will notify the Controller to that effect as soon as possible. The Processor is entitled to suspend the implementation of the appropriate instruction until it is confirmed or adjusted by the Controller.

3. Processor's duties

- 3.1.** The Processor, in its role as a data processor, may correct, adjust, cancel or restrict the processing of data that is processed under the RSA only on, and in accordance with, a properly documented instruction given by the Controller. If and to the extent that, in this respect, a data subject contacts the Processor directly, the Processor will pass this request on to the Controller without undue delay. Each party will work with the other to address any issues raised by data subjects.
- 3.2.** The Processor represents and warrants that it will comply with its duties under Art. 28 to 33 GDPR including but not limited to:
 - 3.2.1.** the duty to appoint a data protection officer where prescribed by law.
 - 3.2.2.** Confidentiality according to Art. 28 subs. 3 b), 29, 32 subs.4 GDPR. The Processor will only engage employees in the performance of the services who have been committed to confidentiality and have been made familiar with the data protection and privacy regulations which are relevant for their work. The Processor as well as any person subordinated to it who has access to personal data may process this data exclusively in accordance with the instructions given by the Controller, including the powers and authorizations granted in this agreement, unless they are obliged by law to process the data. Data secrecy has to be maintained even after the termination of the contract.
 - 3.2.3.** Information on control measures and other measures taken by regulatory authorities must be given to the Controller without undue delay , if and to the extent such measures relate to the RSA. This also applies if and to the extent that a competent authority conducts investigations in the context of proceedings for administrative or criminal offences regarding the processing of personal data in the context of data processing by the Processor on behalf of the Controller.
 - 3.2.4.** If and to the extent that the Controller itself is exposed to control measures by the regulatory authority or to proceedings for administrative or criminal offences or to a claim for information or a liability claim asserted against the Controller by a data subject or a third party or to any other claims relating to the contract data processing by the Processor on behalf of the Controller, the Processor will be obliged to use its best endeavours to support and assist the Controller.
 - 3.2.5.** The parties, upon request, will cooperate with a regulatory authority with jurisdiction and work together to address any issues raised by such regulatory authority.
 - 3.2.6.** The Processor regularly controls its internal processes as well as the technical and organizational measures to ensure that the processing performed under its responsibility is in conformity with the requirements of the applicable data protection and privacy law and that the rights of the data

subject are protected.

- 3.3. The Processor will correct, adjust, cancel or block the data to be processed under the contract upon appropriate request by the Controller.
- 3.4. Upon request by the Controller, data, data media or carriers and any other material must be either returned or deleted after the termination of the contract, subject to the Processor's legal right or necessity to retain information for permitted purposes under the relevant laws.

4. Technical and organizational measures

- 4.1. The Processor, prior to the commencement of the data processing, will document the implementation of the required technical and organizational measures which have been defined and specified prior to entering into the RSA, in particular as regards the details of the specific contract execution, as noted in **Annex B**, and these technical and organizational measures are a primary basis for the RSA. If and to the extent the the Controller requires an adjustment in the technical and organizational measures, such adjustment will be implemented by mutual agreement.
- 4.2. The technical and organizational measures measures to be taken ensure a security level appropriate to the existing risks as regards confidentiality, integrity, availability and resilience of the systems, as detailed in **Annex B**.
- 4.3. The technical and organizational measures are subject to technical progress and further development. The parties are allowed to implement alternative appropriate measures as technology evolves and best practices improve. The Processor will not, however, fall below the security level defined for the agreed measures, and changes to practices will be documented in a revised **Annex B**.

5. Controller's duties

- 5.1. The Controller is responsible for the lawfulness of the collection, processing and use of the Controller's data as well as for the protection of the rights of the data subjects.
- 5.2. The Controller is the owner of the Controller's data and the owner of the rights, if any, relating to the Controller's data.
- 5.3. It is the responsibility of the Controller to provide the Processor with the Controller's data to enable service provision as agreed in the RSA and the Controller is responsible for the quality of the Controller's data. The Controller will inform the Processor without undue delay of any failures, errors or irregularities with the handling of Personal Data.

6. Compliance Documentation and Audit

- 6.1. The Controller, prior to the commencement of data processing and at regular intervals thereafter, understands that the Processor complies with its duties under Art. 28 GDPR and in particular takes all required technical and organizational measures and documents the results. When necessary, the Controller may request information from the Processor about its practices and seek reasonable documentation about such practices.
- 6.2. The Processor is entitled, in its sole discretion and in consideration of the statutory obligations of the Controller, to refuse the disclosure of any information which is critical with regard to the Processor's business or where the disclosure of such information would constitute a violation of statutory or contractual regulations. The Controller will not be granted access to data or information about other customers of the Processor or access to information regarding its costs to any other confidential data of the Processor which is not of direct relevance for the agreed control purposes.
- 6.3. The Controller is obliged to inform the Processor in due time (as a rule at least two weeks in advance) of all circumstances related to the implementation of the control procedure. The Controller, as a rule, is not allowed to carry out more than one control per calendar year. This is without prejudice to the Controller's right to carry out additional controls in the case of special occurrences.

- 6.4. If the Controller engages a third party to carry out the control, the Controller is obliged to create a commitment of such third party in writing which corresponds to the Controller's commitment to the Processor under this § 6. In addition, the Controller is obliged to commit the third party to confidentiality and secrecy unless the third party in question is bound to professional secrecy. The Controller, upon the Processor's request, is obliged to submit to the Processor the appropriate agreements concluded with the third party without undue delay . The Controller is not entitled to engage competitors of the Processor to carry out the controls.
- 6.5. The Processor, at its choice and instead of an on-site control, may also prove compliance with the technical and organizational measures according to **Annex B** by submitting proof of compliance with authorized rules of conduct according to Art. 40 GDPR or by equivalent means, provided that the mechanism enables the Controller to reasonably satisfy itself that the technical and organizational measures according to **Annex B** to this agreement are duly implemented.

7. Sub-Processors

- 7.1. The Controller agrees that the Processor, in order to provide the services stipulated by the RSA, will involve companies affiliated with the Processor to perform such services, or engage companies as Sub-Processors to perform the agreed services. The Processor will carefully select the Sub-Processors by their qualification and suitability.
- 7.2. The Processor is allowed to engage Sub-Processors and/or change existing Sub-Processors if and to the extent that (a) the Processor notifies the Controller of the intended subcontracting/outsourcing in writing, including by supplementing **Annex C** to this DPA, within a reasonable time prior to services going live, and (b) the subcontracting is based on a contractual agreement according to Art. 28 subs. 2 – 4 GDPR.
- 7.3. The Processor is allowed to engage third-party registries, and their agents (as necessary), to provide the services under the RSA. In the event that a third-party registry does not comply with Data Processing Laws, this fact will be disclosed to a User prior to any collection or processing of Personal Data, gathering appropriate consent.
- 7.4. Only after all conditions for the subcontracting have been fulfilled, the Processor will be allowed to disclose personal data of the Controller to the Sub-Processor and the Sub-Processor will be allowed to provide the agreed services for the first time.
- 7.5. As of the time of conclusion of this agreement, the companies listed in **Annex C** are currently engaged by the Processor as Sub-Processors to perform parts of the services to be provided and, in this context, they also directly process and/or use the data of the Controller. The Controller hereby consents to the engagement of these Sub-Processors.
- 7.6. If the Processor engages Sub-Processors, the Processor is responsible for imposing on the Sub-Processor the same duties which the Processor has under the present agreement with regard to data protection and privacy law.
- 7.7. Subcontracting does not require consent by or notice to the Controller if the Processor engages third parties for the purposes of ancillary services related to the main services such as in the case of external personnel, postal and dispatch services, maintenance or user service. The Processor will conclude agreements with such third parties to the extent required to ensure adequate data protection and privacy and data security and to enable control measures.

8. Notification of breaches by the Processor

- 8.1. The Processor supports and assists the Controller in complying with the duties under Articles 32 to 36 GDPR to ensure the security of personal data, the duty to report breaches reportable under the GDPR, and any data protection impact assessments as the need arises. This includes among other things: (a) ensuring adequate security standards through the technical and organizational measures which take into account the circumstances and purposes of data processing and the anticipated likelihood and severity of a possible data breach; (b) informing Controller of any reportable breaches

of personal data under the GDPR to the Controller without undue delay; (c) supporting and assisting the Controller in its duty to inform data subjects and, in this context, provide the Controller with all relevant information without undue delay; (d) supporting and assisting the Controller in assessing the data protection impact of activities under the RSA; and (e) supporting and assisting the Controller in prior consultations with any relevant regulatory authority.

9. Deletion and return of personal data

- 9.1.** No copies or duplicates will be generated without the knowledge or an appropriate instruction by the Controller. This does not apply to (a) back-up copies if and to the extent they are required to ensure proper data processing; or (b) data which is required for the purposes of compliance with statutory retention duties, ICANN compliance, or contractual compliance with a third-party registry, all of which form an essential element of the services of the RSA.
- 9.2.** The Processor, no later than upon termination of the RSA or, as the case may be, already upon completion of the contractually agreed services or upon request by the Controller, returns and hands over to the Controller all documents, results generated by the Processor in processing and/or using data as well as all data and databases relating to the contract which are in the Processor's possession, except as retention is expressly allowed under the GDPR.
- 9.3.** Any evidence and documentation which is meant to evidence proper data processing in accordance with the contractual and other applicable requirements must be retained by the Processor even beyond the end of the contract for the applicable retention period. The Processor, to relief itself, may hand over such evidence and documentation to the Controller upon termination of the contract.

10. Information duties, written form clause, choice of law

- 10.1.** If the data of the Controller should be endangered by any seizure or attachment of the Processor's property or by insolvency or composition proceedings or other events or measures taken by third parties, the Processor will be obliged to inform the Controller without undue delay. The Processor will inform all responsible persons and bodies without undue delay to the effect that the Controller is the sole owner of, and has exclusive responsibility for and control over the data.
- 10.2.** Changes and amendments to this Annex or any parts thereof – including any representations and warranties of the Processor – require a legally appropriate new agreement, written notice, and explicit reference to the fact that the change or amendment in question refers to the present DPA.
- 10.3.** In the case of discrepancies or conflicts, the provisions contained in this Annex governing data protection and privacy take precedence over the provisions of the RSA. If the parties have executed multiple data protection agreements, this version takes precedence over the provisions of any other such agreement as it respects the provisioning of the services in the RSA. If any individual parts of this Annex should be invalid, this will be without prejudice to the validity of the remaining provisions of the Annex.

11. When the Parties are Joint Controllers

- 11.1.** If or when the parties are joint controllers, the parties agree and warrant that the processing of Personal Data has been carried out in accordance with Data Protection Laws applicable to each of them with regards to Personal Data under the RSA.
- 11.2.** If or when the parties are joint controllers, the parties agrees and warrants that (a) they each will process Personal Data solely for the purpose of performing obligations under RSA or any other purpose expressly permitted any agreement either party has with a User and in accordance with applicable Data Protection Laws; (b) they each will deal promptly with all reasonable inquiries from the other party, or from a User, relating to Personal Data, including requests for access or correction of Personal Data and information about relevant practices, procedures and complaints processes; (c)

they each have in place procedures so that third-parties authorized to have access to Personal Data, other than registry providers and their authorized agents, will maintain the confidentiality and security of Personal Data and that any person acting under the authority of such party shall be obligated to process Personal Data only on instructions from the party; and (d) when required under Data Protection Laws, each party will provide prior notice to the other before authorizing any-third party, other than registry providers and their authorized agents, to have access to Personal Data.

- 11.3.** If or when the parties are joint controllers, the parties understand that third-party registries are required to provide services under the RSA. In the event that a third-party registry does not comply with Data Processing Laws, Enom will present this fact to a User prior to any collection or processing of Personal Data, gathering appropriate consent.

Annex A – Standard Contractual Clauses

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

Customer, as identified in Enom Reseller Agreement

- and -

Enom.com Co.
5808 Lake Washington Blvd. NE, Suite 201
Kirkland, WA 98033, USA

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

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

Clause 1: Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

Clause 2 : Details of the Transfer

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

Clause 3 : Third-Party beneficiary clause

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

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

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

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

Clause 4 : Obligations of the Data Exporter

The data exporter agrees and warrants:

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

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

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

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

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

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

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

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

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

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

Clause 5 : Obligations of the Data Importer

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that

request, unless it has been otherwise authorised to do so;

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

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

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

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

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

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

Clause 6 : Liability

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

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

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

under the Clauses.

Clause 7: Mediation and Jurisdiction

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

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

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

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

Clause 8 : Cooperation with Supervisory Authorities

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

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

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

Clause 9: Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely, the jurisdiction named in the Master Services Agreement.

Clause 10 : Variation of the Contract

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

Clause 11 : Sub-processing

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

obligations under such agreement.

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

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely the jurisdiction named in the Master Services Agreement.

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

Clause 12 : Obligation After the Termination of Personal Data-Processing Services

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

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

Clause 13 : Liability

1. The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

2. Indemnification is contingent upon: (a) the data exporter promptly notifying the data importer of a claim; and (b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.

Exhibit 1 to the Standard Contractual Clauses

Data exporter

The company identified in the Master Services Agreement ("RSA") with Enom as "Customer" and which has a services relationship with persons and companies identified in the RSA as "Users", "Registrants", "Registered Name Holders", and/or "Sub-Resellers."

Data importer

The data importer is Enom, as defined in the RSA, which provides those services described in the RSA to permit, provision and maintain the registration of domain names, whois privacy services, digital certificates, and/or domain name service.

Data subjects

The personal data transferred may concern the following categories of data subjects (please specify): the registration and provisioning of Internet domain names, whois privacy services, digital certificates, and/or domain name service.

Categories of data

The personal data transferred concern the following categories of data (please specify): name and appropriate contact information as requested by the relevant top-level domain registry, which includes email address and may also include address, telephone number, and facsimile number.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify): use of contact information as requested by the relevant top-level domain registry for registration at the relevant registry, usage in data escrow services, and publication, when relevant and required, in whois databases.

Annex B – Technical and Organizational Measures

This Technical and Organizational Security Exhibit (Annex B) describes the technical and organizational security controls employed in connection with the Enom services, technical support services and other services specifically provided under the parties' Reseller Agreement ("RSA"). This Exhibit is incorporated by reference into the RSA. Capitalized terms have the meaning stated in the RSA or as defined herein.

1. Confidentiality (Art. 32 subs. 1 b) GDPR)

a. Physical access control.

- i. Enom limits facilities access to authorized individuals. All facilities are locked at all times and require security cards for entrance. Guests are required to sign in and are accompanied by Enom's employees. Facilities entrances and exits are monitored.
- ii. Services infrastructure operated outside the Enom corporate facilities involve similar physical and environmental security controls.
- iii. When Enom uses third-party co-located data centers for provision of the services, Enom requires that the service provider meets or exceeds the physical and environmental security requirements of Enom-managed facilities. Minimum security requirements include: physical access restrictions and safeguards; adequate separation of customer environments; fire suppression, detection, and prevention mechanisms; climate control systems.
- iv. When Enom uses Cloud-Based Infrastructure for provision of services, Enom contracts with providers that provide a materially similar level of physical access control to the service levels described above.

b. Logical access control.

- i. Enom requires that its employees and contractors secure computers and data while unattended.
- ii. Enom uses industry-standard practices to identify and authenticate users accessing its information systems and monitors connections for abuse or unauthorized uses. When authentication is based on passwords, Enom follows industry-standard practices for password handling and management, including length and complexity requirements. Personnel are prohibited from sharing passwords. Enom follows industry-standard practices to deactivate passwords or accounts that have been corrupted or inadvertently disclosed.
- iii. Enom monitors attempts to gain unauthorized access to its systems and services. Enom uses industry standard practices to maintain the confidentiality and integrity of passwords when they are assigned, distributed and stored.

c. Data access control.

- i. Enom restricts access to its systems to only those individuals who require such access to perform their job function.
- ii. Enom maintains a record of security privileges of individuals having access to its systems.
- iii. New access to systems is reviewed and approved by management prior to being granted.
- iv. Enom performs regular reviews of user accounts and assigned permissions for key systems.
- v. Enom limits the personnel who may grant, alter or cancel authorized access to data and resources.

- vi. Enom ensures that when more than one individual has access to systems containing the individuals have separate identifiers.
- d. Data separation control. Enom collection of Personal Data is solely to provide the services under the RSA, and Enom does not use such data for other purposes that would require separate processing.

2. Integrity (Art. 32 subs. 1 b) GDPR)

- a. Data transfer control. Enom requires encrypted connections to its services interfaces between Customer and Enom at all times. Enom uses industry standard encryption mechanisms both for data in transit and at rest.
- b. Data entry control. Enom implements and maintains industry standard mechanisms to enforce access management and data entry controls around the reception and processing of Personal Data, including journaling of dates and times of data entry and the identity of the person or company that initiated the data creation. Such mechanisms can identify when and by whom data was entered, altered or removed, and when necessary, the mechanisms can restore data to previous states.
- c. Event Logging. In performance of the services in the RSA, Enom collects logs. Logs may include access ID, time, authorization granted or denied, diagnostic data, and other relevant activity. Logs are used (i) for providing, securing, managing, measuring and improving the Enom services, (ii) as directed or instructed by Customer and its Users, and/or (iii) for compliance with Enom policies, applicable law, regulation, or governmental request. This may include monitoring the performance, stability, usage and security of the Enom' services.
- d. Deletion Processes. Enom securely deletes Personal Data when no longer needed for a legitimate purpose. Enom may retain Personal Data following the relevant service period where required for legal purposes. Enom will comply with the requirements of this Exhibit until such data has been permanently deleted. Enom is under no obligation to Customer to retain Personal data, or any data of Customer or its Users, following termination of the RSA. Return.

3. Availability and resilience (Art. 32 subs. 1 b) GDPR)

- a. Availability Control. Enom' services are maintained in high availability clusters spanning multiple physical sites. All databases are backed up and maintained using at least industry standard methods, and data required for domain name services are stored redundantly in escrow, as mandated by certain contracts with third-party registries and ICANN.
- b. Failover Protection. Enom implements mechanisms designed to address loss of availability of data, including storing copies of data in a different place from where the primary computer equipment processing such is located.
- c. Intrusion Control. Enom uses anti-virus software, malware monitoring software, and other industry-standard controls to avoid malicious software gaining unauthorized access to Personal Data, including malicious software originating from public networks or from Customer.
- d. Prevention, Detection and Escalation Control. Enom uses both industry-standard mechanisms and proprietary mechanisms to prevent intrusions and data breaches and to maintain data integrity. It routinely monitors its systems for non-normal activities, and it has established escalation paths for any data disruptions to appropriate personnel.

- e. Restoration of Availability. Enom is capable of restoring all data used in its services from back-up, typically without an interruption in service. Data for services also can be restored from third-party escrow, either to Enom or a successor registrar, if necessary and appropriate.

4. Processes for regular testing, assessment and evaluation (Art. 32 subs. 1 d) GDPR; Art. 25 subs. 1 GDPR)

- a. Monitored Security Controls. Enom has appointed one or more security and technical officers responsible for coordinating and monitoring security controls for the services it provides under the RSA.
- b. Confidentiality Obligations. Enom personnel and all third-party contractors with access to Personal Data and data of the Customer are subject to confidentiality obligations.
- c. Personnel and Policy. Enom maintains a systems engineering team responsible for implementing and communicating to the company the overarching security and safety principles established and approved by executive management. Policies provide security requirements in a clear and concise manner. Standards define the process or methodology of meeting policy requirements.
- d. Regular Assessments. Enom routinely performs assessments of key areas of risk associated with the services provided under the RSA including, by way of example only and as applicable, privacy risk assessments, open source reviews, and contractual compliance reviews.
- e. Contract Reviews. Enom reviews all new and renewing contracts against data protection laws, including the GDPR, and selects and retains only those vendors that commit to similar levels of security and data protection. Service providers that may access Personal Data subject to European Union law are required to self-certify to EU-U.S. and EU-Swiss Privacy Shield programs or to execute Standard Contractual Clauses.
- f. Service Provider Review and Termination. Service providers are assessed periodically based upon the sensitivity and risk associated with their services. Upon termination of a supplier relationship, the service provider is required to return all or certify the secure destruction of all Personal Data, if any, in its possession.

Annex C – Sub-Processors engaged by the Processor

The gTLD and ccTLD registries and their agents listed on the “Data Use Information Page,” provided to each User at registration of a domain name and provided inside the User’s domain name account.

The authoritative list of companies and entities that operate TLD registries is maintained by the Internet Assigned Numbers Authority at <https://www.iana.org/domains/root/db>.

The Internet Corporation for Assigned Names and Numbers (“ICANN”)

Iron Mountain Data Escrow Services

DENIC Data Escrow Services

ZenDesk

American Express

Paypal

Sage (Intacct)

Kibana

Bluesnap

Pentaho