Data Processing Addendum
(Revision May 2018)

Agreement entered into by and between
Customer, as identified in Tucows Master Services Agreement
– "Controller" or "Joint Controller" or "Customer" –

and

Tucows.com Co.
96 Mowat Avenue
Toronto, Ontario
Canada, M6K 3M1
– "Processor" or "Joint Controller" or "Tucows" –

Preamble

This Data Processing Agreement ("DPA") defines and sets out in detail the data protection obligations of the contracting parties arising under the Master Services Agreement ("MSA") entered by the parties. It applies to all activities relating to the MSA 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..

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

1.1. The MSA 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 Tucows' Data Use Information Page. The term and termination of this agreement follows the term and termination agreed upon in the MSA. Termination of the MSA 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 MSA. 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 MSA 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 date processor, may correct, adjust, cancel or restrict the processing of data that is processed under the MSA 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 MSA. 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 MSA, 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 MSA. 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 MSA 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 MSA, 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 MSA. In the event that a third-party

registry does not comply with Data Processing Laws, this face 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 MSA; 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 MSA.

9.2. The Processor, no later than upon termination of the MSA 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 MSA. 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 MSA. 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 MSA.

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 MSA 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 MSA. In the event that a third-party registry does not comply with Data Processing Laws, Tucows 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 Tucows Master Services Agreement

- and -

Tucows.com Co.
96 Mowat Avenue
Toronto, Ontario
Canada, M6K 3M1
+1 (416) 535-0123

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 of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a 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 ("MSA") with Tucows as "Customer" and which has a services relationship with persons and companies identified in the MSA as "Users", "Registrants", "Registered Name Holders", and/or "Sub-Resellers."

Data importer

The data importer is Tucows, as defined in the MSA, which provides those services described in the MSA 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 Tucows' OpenSRS services, technical support services and other services specifically provided under the parties' Master Service Agreement ("MSA"). This Exhibit is incorporated by reference into the MSA. Capitalized terms have the meaning stated in the MSA or as defined herein.

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

a. Physical access control.

- **i.** Tucows limits facilities access to authorized individuals. All facilities all locked at all times and require security cards for entrance. Guests are required to sign in and are accompanied by Tucows' employees. Facilities entrances and exits are monitored.
- **ii.** Services infrastructure operated outside the Tucows corporate facilities involve similar physical and environmental security controls.
- **iii.** When Tucows uses third-party co-located data centers for provision of the services, Tucows requires that the service provider meets or exceeds the physical and environmental security requirements of Tucows-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 Tucows uses Cloud-Based Infrastructure for provision of services, Tucows contracts with providers that provide a materially similar level of physical access control to the service levels described above.

b. Logical access control.

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

c. Data access control.

- i. Tucows restricts access to its systems to only those individuals who require such access to perform their job function.
- ii. Tucows 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. Tucows performs regular reviews of user accounts and assigned permissions for key systems.
- v. Tucows limits the personnel who may grant, alter or cancel authorized access to data and resources.
- vi. Tucows ensures that when more than one individual has access to systems containing the individuals have separate identifiers.

d. Data separation control. Tucows collection of Personal Data is solely to provide the services under the MSA, and Tucows 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. Tucows requires encrypted connections to its services interfaces between Customer and Tucows at all times. Tucows uses industry standard encryption mechanisms both for data in transit and at rest.

b. Data entry control. Tucows 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 MSA, Tucows 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 Tucows services, (ii) as directed or instructed by Customer and its Users, and/or (iii) for compliance with Tucows policies, applicable law, regulation, or governmental request. This may include monitoring the performance, stability, usage and security of the Tucows' services.

d. Deletion Processes. Tucows securely deletes Personal Data when no longer needed for a legitimate purpose.Tucows may retain Personal Data following the relevant service period where required for legal purposes. Tucows will comply with the requirements of this Exhibit until such data has been permanently deleted. Tucows is under no obligation to Customer to retain Personal data, or any data of Customer or its Users, following termination of the MSA. Return.

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

a. Availability Control. Tucows' 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. Tucows 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. Tucows 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. Tucows 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. Tucows 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 Tucows 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. Tucows has appointed one or more security and technical officers responsible for coordinating and monitoring security controls for the services it provides under the MSA.

   b. Confidentiality Obligations. Tucows 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. Tucows 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. Tucows routinely performs assessments of key areas of risk associated with the services provided under the MSA including, by way of example only and as applicable, privacy risk assessments, open source reviews, and contractual compliance reviews.

   e. Contract Reviews. Tucows 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

Bluesnap

Pentaho