Exhibit A
RRA Data Processing Addendum

To the extent of any conflict between the Agreement's other sections (including any of its exhibits or attachments), and this Data Processing Addendum, the terms of this Data Processing Addendum will take precedence. Capitalized terms not defined below will have the meaning provided to them in the Agreement (also referred to in this Data Processing Addendum as, the "**RRA**").

~~1.~~ 1. INTRODUCTION

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

~~2.~~ 2. DEFINITIONS

a) Alternative Transfer Solution. Means a mechanism other than the Applicable Standard Contractual Clauses that enables the lawful transfer of Shared Personal Data from the EEA, UK, or Switzerland to a third country in accordance with Applicable Data Protection Laws, including as applicable, the Swiss-U.S. or UK-U.S. Privacy Shield self-certification programs approved and operated by the U.S. Department of Commerce ("**Privacy Shield**") or another valid certification program in force under Applicable Data Protection Laws.

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

~~b)~~ c) Applicable ~~Laws. The General Data Protection Regulation (2016/679) ("GDPR"), the Electronic Communications Data Protection Directive (2002/58/EC), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) (as amended) and all other applicable~~ Data Protection Laws. Means all privacy, data security, and data protection laws ~~and~~, directives, regulations ~~worldwide, including their successors or as modified, relating~~, or rules in any jurisdiction applicable to ~~the~~ Your Processing of Shared Personal Data, including the GDPR, CCPA, HIPAA, and LGPD.

d) Applicable Standard Contractual Clauses. Means the European Commission's standard contractual clauses which are standard data protection terms for the transfer of personal data to third countries that do not ensure an adequate

level of data protection, as described in Article 46 of the EU GDPR including: (i) Controller-Processor SCCs, (ii) UK Controller-Processor SCCs, (iii) Controller-Controller SCCs, or (iv) the UK Controller-Controller SCCs, each as defined in this Data Processing Addendum.

e) CCPA. Means, as applicable: (i) the California Consumer Privacy Act of 2018, California Civil Code 1798.100 et seq. (2018); (ii) the California Privacy Rights Act of 2020, and (iii) Applicable Data Protection Laws modeled on either of the foregoing.

f) Controller-Controller SCCs. Means the terms at https://business.safety.google/gdprcontrollerterms/sccs/eu-c2c.

g) Controller-Processor SCCs. Means the terms at https://business.safety.google/gdprcontrollerterms/sccs/eu-c2p-ipa.

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

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

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

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

l) GDPR. Means (i) the European Union General Data Protection Regulation (EU) 2016/679 (the "**EU GDPR**") on data protection and privacy for all individuals within the European Union ("**EU**") and the European Economic Area ("**EEA**"); (ii) the EU GDPR as incorporated into United Kingdom ("**UK**") law by the Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("**UK GDPR**"); and (iii) the Federal Data Protection Act of 19 June 1992 (Switzerland) (each as amended, superseded, or replaced).

m) Google Controller. Means the Google Entity that Processes Personal Information as a Data Controller in accordance with Google's applicable privacy policy.

n) LGPD. Means Brazilian Law no. 13,709 for the protection of personal data.

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

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

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

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

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

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

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

v) UK Controller-Controller SCCs. Means the terms at https://business.safety.google/gdprcontrollerterms/sccs/uk-c2c.

w) UK Controller-Processor SCCs. Means the terms at https://business.safety.google/gdprcontrollerterms/sccs/uk-c2p-ipa.

3. 3. PURPOSE, SUBJECT MATTER, AND ROLES

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

b) b) Subject Matter. This Data Processing Addendum sets out the framework for the protection of Shared Personal Data for the Purposes noted in this

section and defines the principles and_ procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other. The Parties collectively acknowledge and agree that Processing necessitated by the Purpose(s) _is to be performed at different stages, or at times even simultaneously by the Parties. Thus, this_ Data Processing Addendum is required to ensure that where Shared Personal Data may be _Processed, it is done so at all times in compliance with the requirements of Applicable Data_ Protection Laws.

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

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

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

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

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

4. 4. FAIR AND LAWFUL PROCESSING

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

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

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

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

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

iv. iv. Processing is necessary for the purposes of the legitimate interests pursued by the _Controller or by a third party, except where such interests are overridden by the interests _or fundamental rights and

freedoms of the Data Subject which require protection of Personal Data; or

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

~~5.~~ 5. PROCESSING SHARED PERSONAL DATA

~~a)   All Parties agree that they are responsible for Processing of~~

a) Data Transfers. Each Party may transfer Shared Personal Data ~~in accordance with~~if it complies with applicable provisions on the transfer of Shared Personal Data required by Applicable Data Protection Laws~~and this Data Processing Addendum. The Parties shall fully cooperate with each other to~~.

i. To the extent ~~necessary to effectuate corrections, amendments, restrictions or deletions of Personal Data as required by Applicable Laws and/or at the request of any Data Subject.~~

~~b) A Party may only transfer~~a Party transfers Shared Personal Data relating to individuals within the UK, EEA, or Switzerland to the other Party and the receiving Party is not: (i) subject to the binding obligations of a valid Alternative Transfer Solution, or (ii) located in a jurisdiction that is subject to a valid adequacy decision (as determined by the Applicable Data Protection Laws regarding the individuals about whom the Shared Personal Data is Processed), You and Google expressly agree to the Applicable Standard Contractual Clauses including the warranties and undertakings contained therein as the "data exporter" and "data importer" as applicable to the transfer contemplated by the Parties.

ii. To the extent Section 5(b)(i) applies and You Process Shared Personal Data as a Data Processor: (i) if Google transfers Shared Personal Data relating to ~~EU~~individuals ~~to outside of the European Economic Area ("EEA")~~within the EEA or Switzerland to You, You and Google (on its own behalf or on behalf of the Google Controller) agree to the Controller-Processor SCCs; and (~~or~~ii) if ~~such~~Google transfers Shared Personal Data ~~is already outside of the EEA, to any third party also outside the EEA), in compliance with the terms of this Data Processing Addendum and the requirements of Applicable Laws, the latter including any relevant Adequacy Decision of the European Commission or the use of EU 'Standard Contractual Clauses'.~~ ==~~Where Standard Contractual Clauses for data transfers between EU and non-EU countries are required to be executed between the Parties, they may be found and downloaded, to be incorporated herein as part of this Data Processing Addendum upon execution, at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32 010D0087 (or such link location as may be updated from time to time).==~~ relating to individuals within the UK to You, then You and

Google (on its own behalf or on behalf of the Google Controller) agree to the UK Controller-Processor SCCs.

iii. To the extent Section 5(b)(i) applies and You Process Shared Personal Data as a Data Controller: (i) if Google or You transfer Shared Personal Data relating to individuals within the EEA or Switzerland to the other Party, You and Google (on its own behalf or on behalf of the Google Controller) agree to the Controller-Controller SCCs; and (ii) if Google or You transfer Shared Personal Data relating to individuals within the

UK to the other Party, then You and Google (on its own behalf or on behalf of the Google Controller) agree to the UK Controller-Controller SCCs.

iv. To the extent either Party Processes Shared Personal Data transferred in accordance with an Alternative Transfer Solution, the Party receiving Shared Personal Data will: (i) provide at least the same level of protection for the Shared Personal Data as is required by the Applicable Agreements and the applicable Alternative Transfer Solution; (ii) promptly notify the Party disclosing Shared Personal Data in writing if the receiving Party determines that it can no longer provide at least the same level of protection for the Shared Personal Data as is required by the Applicable Agreements and applicable Alternative Transfer Solution; and (iii) upon making such a determination, cease Processing Shared Personal Data until the Party receiving Shared Personal Data is able to continue providing at least the same level of protection as required by the Applicable Agreements and the applicable Alternative Transfer Solution.

v. Google LLC has certified under the Privacy Shield on behalf of itself and certain wholly-owned US subsidiaries, including Google. Google LLC's certification and status is available at https://www.commerce.gov/page/eu-us-privacy-shield.

vi. Where Google is not the Google Controller, Google will ensure that it is authorized by the Google Controller to (i) enter into the Applicable Standard Contractual Clauses on behalf of the Google Controller, and (ii) exercise all rights and obligations on behalf of the Google Controller, each as if it were the Data Controller.

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

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

confidentiality agreement to maintain the confidence of the Shared Personal Data.

e) d) Where a Party Processes Shared Personal Data, it acknowledges and agrees that it is responsible for maintaining appropriate organizational and security measures to protect such Shared Personal Data in accordance with all Applicable Data Protection Laws. Appropriate organizational and security measures are further enumerated in Section 56 of this Data Processing Addendum, but generally must include:

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

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

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

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

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

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

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

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

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

i) h) The Parties shall, in respect of Shared Personal Data, ensure that their privacy

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

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

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

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

6. SECURITY

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

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

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

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

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

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

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

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

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

implementation, and the state of the art;

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

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

7. 7. SECURITY BREACH NOTIFICATION

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

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

i. i. A description of the nature of the incident and likely consequences of the incident; ii. ii. Expected resolution time (if known);

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

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

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

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

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

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

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

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

8. 8. DATA SUBJECT RIGHTS

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

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

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

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

9. 9. DATA RETENTION AND DELETION

Notwithstanding any requirements under the Applicable Agreements to the contrary, the

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

10. 10. TRANSFERS

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

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

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

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

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

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

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

11. 11. RESOLUTION OF DISPUTES

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

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

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

12. 12. IMPACT OF CHANGES; NEW GUIDANCE

In the event the ICANN Board adopts changes to the Temporary Specification (a

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

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

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

Annex 1

DETAILS OF THE PROCESSING

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

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

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

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

Document comparison by Workshare on Wednesday, March 9, 2022 6:33:52 PM

Input:	
Document 1 ID	Old Google Registry RRA DPA
Description	originalDocument
Document 2 ID	New RRA DPA
Description	modifiedDocument
Rendering set	standard

Legend:	
Insertion	
~~Deletion~~	
~~Moved from~~	
Moved to	
Style change	
Format change	
~~Moved deletion~~	
Inserted cell	
Deleted cell	
Moved cell	
Split/Merged cell	
Padding cell	

Statistics:	
	Count
Insertions	337
Deletions	141
Moved from	3
Moved to	3
Style changes	0
Format changes	0
Total changes	484