GoDaddy Registry

RDAP Access Policy

9 February 2022

This document is provided pursuant to the disclaimer provided on the last page.

Contact

Title	Customer Support
Phone	+1 480 651 9999
Email	help@registry.godaddy

Classification

Public - GoDaddy Registry © 2022

Definitions

Anonymous User means any user that is not an Authenticated User.

Authenticated User means a credentialed user logged into the Service using a username, password and digital certificate issued by us.

ICANN means the Internet Corporation for Assigned Names and Numbers, its successors and assigns.

RDAP means the Registry Data Access Protocol, a JSON based protocol intended to replace the WHOIS protocol.

Registry Operator means the entity authorised by ICANN to operate a TLD.

Service means the RDAP services that we provide.

TLD means any Top Level Domain for which we provide the Service.

We, us and our means Registry Services, LLC ("GoDaddy Registry") or our designated representatives.

You and your means the person or entity receiving or accessing the Service.

Purpose

The purpose of this policy is to describe how users may access and use the Service, and what action may be taken by us in the event that we detect behaviours that are not consistent with this policy.

Audience

RDAP Users

Contents

1 Accessing the Service 1
1.1 Authentication 1
1.2 Digital Certificates 1
2 Data Policy 2
2.1 Redacted or Truncated Responses 2
2.2 Result Limits 2
2.3 Wildcard Searches 2
3 Acceptable Use 3
3.1 Terms of Service 3
3.2 Monitoring 4
3.3 Rate Limiting 5
3.4 Suspension of User Authentication 5
4 Definition and Review 6
Exhibit 1 – RDDS Data Protection Addendum 7
Appendix 1 9
Commission Decision C(2004)5721 9
ANNEX A 16
DATA PROCESSING PRINCIPLES 16
ANNEX B 18
DESCRIPTION OF THE TRANSFER 18

1 Accessing the Service

There are two types of access, based on the user:

- Anonymous User Access – any internet user may query the Service, however responses for domain name queries made by Anonymous Users will be redacted.
- Authenticated User Access – by accessing the Service with the necessary credentials (username, password and SSL certificate), Authenticated Users can receive un-redacted responses to queries.

1.1 Authentication

Individuals and organisations with a legitimate interest in accessing domain name registration data may request Authenticated User Access to the Service.

Approved users will be issued a username, password and Registry-signed SSL certificate, allowing them to access the Service as Authenticated Users.

To find out more, or to make a request for access, please visit: RDDSrequest.nic.tld

Note: Replace 'tld' with any of the TLDs supported by GoDaddy Registry.

1.2 Digital Certificates

You will be provided with a Registry-signed SSL certificate that you must use when connecting to the Service as an Authenticated User.

You must ensure that the 'common name' field of the digital certificate must match exactly with the username that will be used when logging in with this certificate. Digital certificates will have a validity period of one (1) year from the date of signing.

It is your responsibility to track the expiry date of your digital certificate(s). You should ensure that you request a new digital certificate from us at least seven (7) days prior to the expiry of your existing digital certificate.

Whilst we will endeavour to remind you that your digital certificate may be expiring, we will not take responsibility for inability to connect to the Service as a result of an expired digital certificate.

Consistent attempts to connect to the Service with an invalid digital certificate may result in the source IP address being blocked at the network level.

2 Data Policy

2.1 Redacted or Truncated Responses

Responses may be redacted or truncated for the following reasons:

- Anonymous User query – contact data is redacted in responses for domain name queries made by Anonymous Users.
- Authenticated User – contact data is not redacted in responses for domain name queries made by Authenticated Users.

2.2 Result Limits

Where a query returns a number of results, the result set will be limited to 20 responses.

Should an Authenticated User have a legitimate purpose for accessing a large number of responses, they may request that we provide the full results.

To make a request, please contact Customer Support with the details of your query and the reason you require access to the unrestricted data set.

2.3 Wildcard Searches

Wildcard searches are not supported.

3 Acceptable Use

As a user of our Service, you agree that you will not use, and you will not permit others to use, the Service we provide in a manner that is:

- for any unlawful, invasive, infringing, defamatory or fraudulent purpose;
- inconsistent with any applicable laws, or to engage in, promote or encourage illegal activity;
- in violation of the legal rights of others, nor to or encourage such violation;
- in contravention of any guidelines and/or policy issued by us from time to time;
- to purposefully distribute any virus, worm, corrupted file, harmful computer code, or other items of a destructive or deceptive nature;
- to modify, affect, disable or circumvent any aspect of the Service or the use of the Service;
- to generate, distribute, or facilitate unsolicited mass email, promotions, advertisings or other solicitations;
- to disrupt the Service or any third party service that may use the Service;
- to alter, steal, corrupt, disable, destroy, trespass or violate any security or encryption of any computer file, database or network; or
- to facilitate any of the above.

3.1 Terms of Service

The Service offered by us is provided for informational purposes only and is designed to assist a user to look up certain information related to the registration records of existing domain names.

The information provided by the Service is 'as is' and we make no guarantee of its accuracy. We cannot, under any circumstances, be held liable in such instances where the stored information would prove to be wrong, incomplete, or not accurate in any sense.

By using the Service you agree to abide by the terms of the Data Protection Agreement, which can be found at Exhibit 1 to this policy.

By submitting a query, you agree that you will not use this data:

1 to allow, enable or otherwise support in any way the transmission of unsolicited, commercial advertising or other solicitations whether via direct mail, email, telephone or otherwise;

2 to enable high volume, automated, electronic processes that apply to the Service or associated systems;

3 for targeted advertising in any possible way;

4 to cause nuisance in any possible way to individuals by sending (whether by automated, electronic processes capable of enabling high volumes or other possible means) messages to them;

5 in a way that is inconsistent with any applicable laws rule, regulation or statute or any policy issued by us; and/or

6 in contravention of any applicable data and privacy protection acts.

Without prejudice to the above, the copying, compilation, repackaging, dissemination or other use of the information provided by the Service is explicitly forbidden without our prior and explicit permission.

If you have been provided with credentials to allow you to access the Service as an Authenticated User, you must not share these with any other person or entity, or allow any other user to access the Service using the credentials provided to you.

By your use of the Service you agree to abide by these Terms of Service and accept that we can take measures to limit the use of the Service in order to protect the privacy of registrants or the integrity of the Service. We may restrict, suspend or terminate your access to the Service at any time. We reserve the right to make changes to the Service and these Terms of Service at any time without prior notice to you. It is your responsibility to review these Terms of Service each time you access or use the Service to keep apprised of any changes. If you do not agree to the changes implemented by us, your sole and exclusive remedy is to terminate your use of the Service.

By executing a query, in any manner whatsoever, you agree to abide by these Terms of Service.

3.2 Monitoring

Where a user is acting in a manner that is considered, in our sole opinion, to be detrimental to the operation of the Service or in contravention of this policy, we may, at our discretion, take action. Such action may include, but not be limited to:

- Limiting the type or number of queries a user may make;
- Restricting the data a user may access;
- Removing access to the Service;
- Where required to do so, report such failure to comply to any law enforcement, government or quasi-governmental agencies, or regulatory bodies.

You should notify us if you intend to perform, in any one twenty four (24) hour period, an increased number of queries than typical. In your request for such, you should indicate if the increase will be one off or, be a permanent increase in query volume.

Any user who significantly increases the number of queries made without prior notification and approval from us may, in our sole discretion, be subject to restrictions as described above.

3.3 Rate Limiting

Queries to the Service may be restricted.

Any user is able to query the Service within the following parameters:

Timeframe	Limit per IP Address
Per Hour	100

Authenticated Users may not be subject to these limits, at our sole discretion.

Result of exceeding the defined limits

Once the configured query limit has been reached the source IP address or address range will be 'black listed' for a period of twenty four (24) hours.

Any source IP address, whether belonging to you or not, that proceeds to perform WHOIS queries after being black listed may be blocked by network level controls. Repeat offenders may be suspended or banned indefinitely.

3.4 Suspension of User Authentication

Should we in our sole discretion, determine that you have failed to comply with any provision of this Policy, you acknowledge that we may restrict, suspend or terminate your access to the Service.

We are not required to give reasons for action taken but may do so from time to time where we deem appropriate at our absolute discretion.

Users may be suspended as a result of any change in:

- A policy of an entity responsible for regulating the domain name system, including ICANN; or
- At the request of a Registry Operator.

If you believe that we have suspended your access to the Service in error, please contact Customer Support.

4 Definition and Review

This document has been prepared and published in order to represent our policy with regard to the administrative and technical management of the Service.

We may discontinue or amend any part or the whole of this policy from time to time at our absolute discretion.

To the extent of any inconsistency with any Registry Operator published policy, this policy shall prevail to the extent of such inconsistency with regards to the RDAP Service only.

Exhibit 1 – RDDS Data Protection Addendum

This Data Protection Addendum (the "DPA") is governs your use of data accessed via a Registration Data Directory Services (RDDS) system offered or operated by Registry Services, LLC ("GoDaddy Registry"), its affiliates, and/or its Registry Operator customers.

By accessing a RDDS data directory offered or operated by GoDaddy Registry, you represent and warrant that you have a legitimate and proportionate interest, consistent with applicable law, to access RDDS data for a specified purpose as identified in Annex B.

You acknowledge that RDDS queries may return personal data that must be protected to ensure respect for the interests and fundamental rights and freedoms of the individual(s) to whom that information relates and to comply with applicable law, including EU Data Protection Law.

NOW, THEREFORE, in consideration of the mutual promises set forth in the Agreement, the Parties hereby agree as follows:

1. Definitions. In this DPA, the following terms shall have the following meanings:

   (a) "Agreement" means the Terms of Service for access to a GoDaddy Registry RDDS;

   (b) "controller", "processor", "data subject", "personal data", and "processing" (and "process") shall have the meanings given in EU Data Protection Law;

   (c) "EU Data Protection Law" means the EU General Data Protection Regulation (Regulation 2016/679); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any national data protection laws in effect made under or pursuant to (i), (ii) or (iii);

   (d) "Relevant Data" means any personal data you receive in response to a RDDS query.

2. Relationship of the Parties. You acknowledge that you act as a separate controller of the personal data you process in connection with the Agreement, and that as a data controller you are responsible for compliance with EU Data Protection Law for the Relevant Data.

3. Transparency and Lawful Processing Obligations. You will maintain a privacy policy that meets the transparency requirements of EU Data Protection Law. You shall process Relevant Data only with a valid lawful basis under law, including EU Data Protection

Law where applicable, and obtain all necessary rights, consents and permissions to process the Relevant Data as a data controller, where necessary.

4. Security. You will implement appropriate technical and organizational measures designed to protect the Relevant Data (a) from accidental or unlawful destruction, and (b) loss, alteration, unauthorized disclosure of, or access to the Relevant Data (a "Security Breach"). In the event that you suffer a Security Breach of the Relevant Data that is likely to result in a high risk to the rights and freedoms of natural persons, you shall notify GoDaddy Registry without undue delay and the parties shall cooperate in good faith to enact such measures as may be necessary to mitigate or remedy the effects of the Security Breach.

5. Subcontracting. You may appoint third party processors to process the Relevant Data, provided that the relationship between you and the processor is based on a contractual agreement that meets the requirements of EU Data Protection Law.

6. Transfer of Data outside the EEA. You may not transfer any Relevant Data to a territory outside of the European Economic Area ("EEA") unless it has complied with EU Data Protection Law in relation to such transfer. Unless you have certified compliance with the EU-US Privacy Shield framework, the standard contractual clauses attached hereto apply to and govern any such transfer. You may transfer data to a third party only where the third party (a) resides or is established in the EEA, (b) has certified compliance with the EU-US Privacy Shield framework, or (c) has executed standard contractual clauses adopted by the European Commission. You, the user (as "data importer"), and GoDaddy Registry (as "data exporter") hereby enter into the Standard Contractual Clauses in respect of any applicable transfer of Relevant Data between you and GoDaddy Registry attached hereto as Appendix 1.

7. Data Disposal. You shall return Relevant Data to GoDaddy Registry and/or delete Relevant Data upon GoDaddy Registry's request.

8. Term. This Addendum shall apply for so long as you process Relevant Data.

9. Indemnification. You shall be liable for and indemnify and hold harmless GoDaddy Registry, its officers, directors, employees, contractors, and agents from and against all claims, suits, judgments, actions, investigations, liabilities, settlements, penalties, fines, damages and losses, demands, costs, expenses, and fees including legal fees and expenses, which arise directly or indirectly out of or in connection with User's data processing activities under the Agreement or the DPA, including, without limitation, those arising out of any third party demand, claim or action, including by a data protection authority, or any breach of contract, negligence, fraud, willful misconduct, breach of statutory duty or non-compliance with any applicable EU Data Protection Law.

10. Governing Law. Unless otherwise required by the Standard Contractual Clauses referred to in Appendix 1, this DPA shall be governed by the laws in the country in which Data Exporter is established.

11. Execution. Use of any RDDS offered or operated by GoDaddy Registry constitutes acceptance of this Addendum.

Appendix 1

EUROPEAN COMMISSION

DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship

Unit C.3: Data protection

Commission Decision C(2004)5721

SET II

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

between

Registry Services, LLC (GoDaddy Registry)

14455 N. Hayden Rd
Suite 100
Scottsdale AZ 85260

hereinafter “data exporter”

and

RDDS USER

hereinafter “data importer”

each a “party”; together “the parties”.

Definitions

For the purposes of the clauses:

a) “personal data”, “special categories of data/sensitive data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby “the

authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

b) "the data exporter" shall mean the controller who transfers the personal data;

c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

Obligations of the data exporter

The data exporter warrants and undertakes that:

a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

I. Obligations of the data importer

The data importer warrants and undertakes that:

a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

h) It will process the personal data, at its option, in accordance with:

i. the data protection laws of the country in which the data exporter is established, or

ii. the relevant provisions[1] of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data[2], or

iii. the data processing principles set forth in Annex A.

i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

i. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

ii. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

iii. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

iv. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

II. Liability and third party rights

a) User shall be liable to GoDaddy Registry, its affiliates and/or its Registry Operator customers for damages it causes by any breach of these clauses. Liability is limited to actual damage suffered. Each party shall be liable to data subjects for damages it causes

[1] "Relevant provisions" means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses).

[2] However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.

by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

III. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

IV. Resolution of disputes with data subjects or the authority

a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the 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) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

V. Termination

a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

b) In the event that:

i. the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

ii. compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

iii. the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

iv. a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

v. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VI. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal

rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.

8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   a) i. such decisions are made by the data importer in entering into or performing a contract with the data subject, and

      ii. the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

   or

   b) where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

Data subjects

The personal data transferred concern the following categories of data subjects:

Domain Name Registrant and their Technical and Administrative Contacts

Purposes of the transfer(s)

The transfer is made for the following purposes:

1. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in user; or

2. The processing is necessary for the purposes of a legitimate interests pursued by user or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection.

Examples of uses that may be permitted, subject to the application of the Principles set out in Annex A, include use of RDDS data to:

- Identify, investigate, and/or resolve technical problems or behaviours that undermine the openness, interoperability, resilience, security and/or stability of the DNS and/or the Internet;
- Resolve disputes regarding the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names);
- Identify, investigate, and/or respond to activities that are potentially deceptive, illegal, malicious or fraudulent;
- Assert, defend, or enforce intellectual property rights;
- Understand the source and reliability of goods or services offered in the online environment; or
- Other uses approved by GoDaddy Registry or a Registry Operator on a case by case basis.

Categories of data

The personal data transferred include name, address, telephone and fax numbers, email addresses.

Recipients

The personal data transferred may be disclosed only to User Affiliates or third parties exclusively for and only as necessary to pursue the legitimate interests for which the Personal Data is sought.

Sensitive data (if appropriate)

None.

Data protection registration information of data exporter (where applicable)

GoDaddy Registry is pending registration with the United Kingdom's Information Commissioner's Office (ICO).

Contact points for data protection enquiries

Data Exporter: privacy@registry.godaddy

Definitions

We, us and our means any or all of Registry Services, LLC ("GoDaddy Registry"), its subsidiary entities and their respective officers, employees, contractors or sub-contractors.

Disclaimer

This document has been produced by us and is only for the information of the particular person to whom it is provided (the Recipient). This document is subject to copyright and may contain privileged and/or confidential information. As such, this document (or any part of it) may not be reproduced, distributed or published without our prior written consent.

This document has been prepared and presented in good faith based on our own information and sources which are believed to be reliable. We assume no responsibility for the accuracy, reliability or completeness of the information contained in this document (except to the extent that liability under statute cannot be excluded).

To the extent that we may be liable, liability is limited at our option to replacing, repairing or supplying equivalent goods or paying the cost of replacing, repairing or acquiring equivalent, or, in the case of services, re-supplying or paying the cost of having such re-supplied.

Confidentiality Notice

This document contains commercially sensitive information and information that is confidential to us. This document is intended solely for the named recipient, and its authorised employees, and legal, financial and accounting representatives (collectively, Authorised Recipients).

The recipients of this document must keep confidential all of the information disclosed in this document, and may only use the information for the purpose specified by us for its use. Under no circumstance may this document (or any part of this document) be disclosed, copied or reproduced to any person, other than the Authorised Recipients, without our prior written consent.

Trademarks Notice

Any of our names, trademarks, service marks, logos, and icons appearing in this document may not be used in any manner by recipients of this document without our prior written consent. All rights conferred under law are reserved.

All other trademarks contained within this document remain the property of their respective owners, and are used only to directly describe the products being provided by them or on their behalf. Their use in no way indicates any relationship between us and the owners of those other trademarks.

Pricing Notice

Any information or pricing provided in this document is subject to change without notice. Whilst we have compiled this document in good faith, based on what we believe is accurate and up-to-date information, it is possible that the pricing or other information contained in this document may require amendment due to changing market or other circumstances (including product discontinuation, manufacturer price changes, errors, or insufficient or inaccurate information having been provided by the recipient of this document or others, and other external circumstances). Additional charges may also apply for work that is out of scope.

The pricing in this document is based on our standard terms and conditions and is valid for a period of thirty (30) days from the date of this document.