.LUXE Policy Overview and Definitions

These Policies Include:

- Overview, including Definitions
- The Sunrise Dispute Resolution Policy (SDRP)
- Naming Policy
- Acceptable Use Policy (AUP)
- Complaint Resolution Service
- Privacy Policy

Overview

The above-stated policies, which in addition to the Registry-Registrant Agreement, govern the top-level domain (TLD or Registry), are based on policies and best practices drawn from ICANN, WIPO, and other relevant sources, and are written to be consistent with ICANN Consensus Policies. Specifically, the Registry Policies include the following interrelated policies, terms, and conditions (together the "Registry Policies"). The Registry policies form a cohesive framework and must be read in conjunction with one another, as well as with other applicable agreements, policies, laws, and regulations which, taken together, represent the entirety of the obligations and responsibilities with regard to any domain name registration.

Background

The Registry Polices are designed to promote transparent and non-discriminatory rules for the registration of domain names within this TLD, including: fair and competitive pricing and competition at the Registrar level; protection of Registrant data and privacy; adherence by Registrants to the AUP; protection of intellectual property rights; protection of certain terms; prevention of the registration of illegal terms; prevention of violations of the law or abuse of the Domain Name System (DNS), including criminal acts; and to align use of the TLD with the applicable self-regulatory environment.

These polices provide that the TLD may, when necessary, implement Registry-level "Registration suspensions" for AUP violations. The registration and use of a domain is subject at all times to the Registry Polices, which provide the means to address crime, prohibited content, intellectual property abuses and other issues of concern.

Definitions

Abuse Point of Contact: an agent of the Registry appointed to review complaints for compliance with these Registry Policies.

Acceptable Use Policy (or AUP): a policy that describes the types of acceptable uses for domain name registrations.

Applicant: is a natural person, company, or organization in whose name an Application is made.

Application: a request submitted by a Registrar, on behalf of an Applicant, to register a second level Domain Name in the .LUXE TLD.

Blocked Names: a list of Domain Names, appearing on a list of blocked names, which list is subject to additions and modifications from time to time, which are indefinitely unavailable for Registration.

Data Escrow: the process of keeping a copy of critical data, including Whois data, with an independent third party.

Domain Name: an identification string that represents an Internet Protocol resource, usually a server computer hosting a web site, which identification string is to the left of the dot in a URL. E.g., in "nominet.uk", the domain name is "nominet."

Domain Name System (or DNS): the system that helps people find their way around the internet. Every computer on the internet has a unique address, which is a string of numbers, called an "IP address" (IP stands for "Internet Protocol"). Because IP addresses are hard to remember, the DNS makes using the internet easier to navigate by allowing a familiar string of letters (the domain name) to be used instead of the IP address.

Domain Lock: a status code that can be set on a domain name in order to prevent unauthorized, unwanted or accidental changes to the domain name's ownership or technical information. When set, the following actions are prohibited: (i) modification of the domain name, including transferring the domain name; (ii) deletion of the domain name; and (iii) modification of the domain name contact details. Where a Domain Lock is applied, renewal of the domain name is still possible.

EPP (Extensible Provisioning Protocol): an industry standard for how Registrars communicate with Registries.

Escrow Agent: a third party contracted to perform data escrow services for the Registry.

ICANN (the Internet Corporation of Assigned Names and Numbers): the organization that creates the rules for, and ensures the technical stability of, the internet.

ICANN Consensus Policies: domain name–related policies created through ICANN's multi–stakeholder consensus–based consultation process to govern certain actions related to domain names, Whois, and other ICANN-related functions; the current list of ICANN Consensus Polices can be found here.

Identical Match: means that a domain name consists of the complete and identical textual elements of a Trademark Clearinghouse–validated trademark. In this regard: (a) spaces contained within a mark that are either replaced in a domain name by hyphens (and vice versa, as the context allows) or omitted may be disregarded for determining Identical Matches; (b) certain special characters (e.g., "@" and "&") contained within a trademark that are spelled out in a domain name with appropriate words describing it may be disregarded for determining Identical Matches; (c) punctuation or special characters contained within a mark that are unable to be used in a second level domain name may either be (i) omitted or (ii) replaced by spaces, hyphens or underscores and still be considered Identical Matches; and (d) no plural and no "marks contained" (i.e., "brandx" in "brandxproducts") qualify for treatment as Identical Matches.

Identifier: a number assigned by the Registry to a Registrant to uniquely identify the Registrant for the purposes of the Registry's operations and to preserve the Registrant's privacy; an individual's name is not used as an Identifier.

IP (Internet Protocol): the technical protocol that allows computers to find and communicate with each other on the internet.

IP Address: a numerical address for a computer connected to the internet.

Naming Policy: the policy that describes reserved and blocked (prohibited) domain names.

Name Server: the server that maps the domain name to an IP address.

Personal Information: means information about an individual person, including any Registrant, whose identity can reasonably be ascertained from such information, but does not include indexes or aggregations of Personal Information relating to more than one person, such as logfiles, DNS Zone Files, databases or backups. This information may include the name, address, telephone number, and email address of the Registrant. This may include the home address and personal email of the Registrant, if the Registrant uses those as their primary contact information for the domain name.

Premium Name(s): means a Domain Name in the TLD whose wholesale registration and/or renewal price is higher than standard TLD registration pricing;

a Premium Name(s) may be sold during each of the TLD's Launch Periods at higher than standard TLD registration pricing.

Primary Purpose: the reasons for the Registry's collection of Personal Information, which is the storage and maintenance of such information in the Whois database (a copy of which ICANN requires is provided to the Escrow Agent) as required by ICANN, which is searchable and publicly available.

Privacy Policy: a policy document that describes how a Registrant's Personal Information may be used by the Registry and in some cases, third parties.

Prohibited Use: a use of the Domain Name that is illegal or expressly prohibited by the Registry Policies, especially the Acceptable Use Policy.

Registrant: a person, whether an individual or business entity, in whose name a domain name is registered.

Registrant Agreement: the document which Registrars must present to Registrants (as a requirement of the terms of the Registry-Registrar Agreement), and which Registrants must acknowledge and agree to in order to register a domain name; the Registrant Agreement binds Registrants, at the time of initial registration, domain renewal, or domain transfer, to the Registry Policies (which also includes by reference, ICANN-mandated rights protection mechanisms such as the Uniform Rapid Suspension service ("URS"), Uniform Domain Name Dispute Resolution Policy ("UDRP"), and other ICANN Consensus Policies);

Registrar: an entity, accredited by ICANN and under contract with the Registry, through which a business entity or individual may register a domain name.

Registrar Registration Fee: payment by the Registrar to the Registry for registration of a Domain Name.

Registration: a Domain Name submitted by a Registrar on behalf of a Registrant for a specified Term that has been accepted by the Registry. A Registrant is the holder of a registered Domain Name in .LUXE.

Registration Fee: payment by the Registrant to the Registrar for Registration of a Domain Name in the TLD.

Registry: is Minds + Machines Group Limited and/or its subsidiaries or affiliated entities.

Registry Policies: the policy framework governing domain name registrations in the TLD, which includes without limitation the Sunrise Dispute Resolution Policy, Naming Policy, Acceptable Use Policy, Complaint Resolution Service Policy,

Privacy Policy, Registry–Registrar Agreement, Registrant Agreement, ICANN consensus polices, and applicable laws, as amended from time to time.

Registry Related Parties: any natural or juristic person who is or is related to the Registry or the Registrar, including the officers, directors, shareholders, owners, managers, employees, agents, representatives, contractors, affiliates, successors, assigns, and attorneys of either the Registry or a Registrar.

Reserved Names: Domain Names in the TLD that are currently unavailable for registration but which may be released in the future.

Root Servers: the authoritative name servers that serve the DNS root zone; a network of hundreds of servers in many countries around the world.

Shared Registry System (SRS): the system that allows multiple Registrars to register domain names in a Registry.

Sunrise: the exclusive period in which trademark owners may register the Identical Match of their trademark as a Domain Name prior to other launch periods including without limitation general domain name availability in the TLD.

Term: the period of registration of a Domain Name in the TLD. Unless otherwise stated in the TLD Start Up Launch Dates and Phases, the initial Term may be between one (1) and ten (10) years, but registration renewals may extend the Term.

Top Level Domain (or TLD): anything to the right of the final dot in a Domain Name; e.g., ".com", ".net", ".ie".

Trademark Claims Service: the service which gives notice to a prospective Domain Name registrant at the time of registration that the desired Domain Name may infringe a trademark; also provides electronic notice to a trademark rights holder that a domain name is an Identical Match to their trademark or to a previously-adjudicated infringing string has been registered. The prospective Registrant must warrant that: (i) they have received notification that the mark is registered in the Trademark Clearinghouse; (ii) they have received and understood the notice; and (iii) to the best of their knowledge, their Registration and use of the requested Domain Name will not infringe on the rights that are the subject of the notice. If the Domain Name is registered subsequent to the notice being issued and the registrant attesting to its non–infringement, the registrar (through an interface with the Clearinghouse) will notify the mark holder(s) of the registration.

Trademark Clearinghouse (TMCH): the central storage repository of validated (authenticated) trademark rights–related data and information for dissemination

with respect to trademark rights protection mechanisms and other registry-related services; more information can be found at their website.

UDRP (Uniform Domain Name Dispute Resolution Policy): an ICANN Consensus Policy that provides for independent adjudication of trademark-related domain name disputes concerning alleged trademark abuse.

URS (Uniform Rapid Suspension): similar to the UDRP, a complimentary rights protection mechanism that offers a lower-cost, faster path to relief for rights holders experiencing the most clear-cut cases of infringement.

Whois: an ICANN-mandated tool that displays the Registrar, Name Server, and other information for a domain name. Whois information is public and searchable.

WIPO: the World Intellectual Property Organization, an international body responsible for the promotion of the protection of intellectual property throughout the world and historic partner with ICANN for UDRP proceedings.

Zone File: the file on a Root Server that contains the domain name registration information necessary to resolve the domain names to their relevant IP addresses.

Sunrise Dispute Resolution Policy

Sunrise Dispute Resolution Policy

This Sunrise Dispute Resolution Policy (the "SDRP") is incorporated by reference into the Registration Agreement. This SDRP is effective as of August 9, 2018. An SDRP Complaint may be filed against a Domain Name registered during the .LUXE TLD during its sunrise period, until thirty (30) days following the close of the sunrise period.

1. Purpose

Domain names in the .LUXE TLD ("the TLD") can be registered by third parties or reserved by the Registry. This SDRP describes the process and standards that will be applied to resolve challenges alleging that a domain name has been registered, or has been declined to be registered, in violation of the Registry's SDRP criteria. This SDRP will not be applied to Registry-reserved names in the TLD.

2. Applicable Disputes

A registered domain name in the TLD will be subject to an administrative proceeding upon submission of a complaint that the Sunrise Registration was improper under one or more of the following criteria.

a. Improper Sunrise Registration-Trademarks[1]

A complaint under this section shall be required to show by reasonable evidence that a registered domain name in the TLD does not comply with the provisions of the Registry's Sunrise Program. The complaint must prove one or more of the following elements:

i. at time the challenged domain name was registered, the registrant did not hold a trademark registration of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty;
ii. the domain name is not identical to the mark on which the registrant based its Sunrise registration;[2]

---

[1] Applicant Guidebook 4 June 2012, Module 5, Page 8, Article 6.2.4. A dispute under this section also addresses the TLD Criteria from ICANN's Trademark Clearinghouse Rights Protection Mechanism Requirements [published 30 September 2013], Article 2.3.6 and Article 2.3.1.4. The FORUM's SDRP does not interact with (nor instruct) the Trademark Clearinghouse and is limited to adjudicating disputes over the Registry's registration and allocation of domain names during the sunrise period.

[2] For the purposes of analysis of this element, neither the gTLD itself, nor the "dot," shall be considered.

iii. the trademark registration on which the registrant based its Sunrise registration is not of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; or
iv. the trademark registration on which the domain name registrant based its Sunrise registration did not issue on or before the date specified by the Registry in its Sunrise Criteria, if one was specified.

b. SDRP Effective Dates. Any SDRP claim brought under this Policy for domain names registered in the .LUXE TLD shall be brought anytime during its sunrise period, until thirty (30) days following the close of the sunrise period.

3. Evidence and Defenses

a. Evidence

Panelists will review the Registry's Sunrise Criteria, allocation requirements, or community-based eligibility requirements which are required to be submitted with the Complaint, as applicable, in making its decision.

b. Defenses

Harmless error. A Respondent may produce evidence to show that, although the sunrise registration was granted based on submission of the wrong documents, or documents containing an error, the true and correct evidence existed at the time the sunrise registration was applied for and, thus, the registration would have been granted.

4. Remedies

The remedies available to a complainant for a proceeding under this SDRP shall be limited to: Improper Sunrise Registration.

If the Panelist finds that the domain name was improperly registered during the Sunrise period, the sole remedy for a Complaint filed under SDRP 2(a) or SDRP 2(b) shall be cancellation of the registration and return of the cancelled domain name to the pool of available names available for registration in the TLD. If the Complainant independently qualifies to register the domain name, either as a regular or defensive/blocking registrant, such application may be made to the Registry, or registrar, as applicable. In the event an SDRP dispute is brought by an auction bidder for the same domain name, the auction will be suspended until the dispute is resolved.

5. Procedure

a. Dispute Resolution Provider / Selection of Procedure

A Complaint under this SDRP shall be submitted to the FORUM ("FORUM") by submitting the complaint directly to the FORUM. The FORUM will administer the proceeding and select a qualified and eligible Panelist ("Panelist"). The FORUM has established Rules for FORUM's Sunrise Dispute Resolution Policy ("Rules"), setting forth a fee schedule and other technical and process requirements for handling a dispute under this SDRP. The proceedings under this SDRP will be conducted according to this SDRP and the applicable Rules of the FORUM.

b. Registry's or Registrar's Involvement

Neither the Registry nor registrar will participate in the administration or conduct of any proceeding before a Panelist. In any event, neither the Registry nor the registrar is or will be liable as a result of any decisions rendered by the Panelist. Any sunrise-registered domain names in the TLD involved in a SDRP proceeding will be locked against transfer to another domain name holder or another registrar during the course of a proceeding.[3] In the case of a claim under SDRP 2(c), the Registry will prevent other parties from registering the unregistered domain name at issue until a decision is reached. The contact details of the holder of a registered domain name in the TLD, against which a complaint has been filed, will be as shown in the registrar's publicly available Whois database record for the relevant registrant. The Registry and the applicable registrar will comply with any Panelist decision and make all appropriate changes to the status of the domain name registration(s) in their Whois databases.

c. Parties

The registrant of a registered domain name in the TLD shall be promptly notified by the FORUM of the commencement of a dispute under this SDRP, and may contest the allegations of the complaint or show other cause why the remedy requested in the complaint should not be granted in accordance with this SDRP. In all cases, the burden of proof shall be on the complainant, and default or other failure of the holder of the registered domain name shall not constitute an admission to any allegation of the complaint. The FORUM shall promptly notify all named parties in the dispute, as well as the registrar and the Registry of any decision made by a Panelist.

---

[3] A Registry may, though its agreement with registrars, instead require the registrar to perform the lock and/or implementation steps.

d. Decisions

(i) The Panelist may state the basis on which the decision is issued in summary format and may include such commentary or guidance as the Panelist deems appropriate;

(ii) the decision shall state whether a registered domain name in the TLD is to be cancelled or the status quo maintained; and

(iii) decisions made under this SDRP will be publicly published by the FORUM on its website.

e. Implementation of a Lock and the Decision

If a Panelist's decision requires a change to the status of a registered domain name, the Registry[4] will wait ten (10) business days after communication of the decision before implementing that decision, unless the registrant submits to the Registry (with a copy to the FORUM) during that ten (10) day period official documentation (such as a copy of a complaint, file-stamped by the clerk of the court) that the registrant has commenced a lawsuit to preserve its claimed rights in a court of competent jurisdiction over the parties and the registered domain name. If such documentation is received no further action shall be taken until the Registry receives (i) evidence satisfactory to the Registry of an agreed resolution between the parties; (ii) evidence satisfactory to Registry that registrant's lawsuit has been dismissed or withdrawn; or (iii) a copy of an order from such court dismissing such lawsuit or otherwise directing disposition of the registered domain name.

f. Representations and Warranties Parties to a dispute under this SDRP shall warrant that all factual allegations made in the course thereof are true and correct to the best of their knowledge, shall remain subject to all representations and warranties made in the course of registration of a disputed domain name.

6. Maintaining the Status Quo

During a proceeding under the SDRP, the registered domain name shall be locked against transfers between registrants and/or registrars and against deletion by registrants.

7. Indemnification / Hold Harmless

The parties shall hold the registrar, the Registry, the FORUM, and the Panelist

[4] A Registry may, though its agreement with registrars, instead require the registrar to perform the lock and implementation steps.

harmless from any claim arising from operation of the SDRP. Neither party may name the registrar, the Registry, the FORUM, or the Panelist as a party or otherwise include the registrar, the Registry, the FORUM, or the Panelist in any judicial proceeding relating to the dispute or the administration of the SDRP policy. The parties shall indemnify, defend and hold harmless the registrar, the Registry, the FORUM, the Panelist and their respective employees, contractors, agents and service providers from any claim arising from the conduct or result of a proceeding under this SDRP. Neither the registrar, the Registry, FORUM, the Panelist and their respective employees, contractors, agents and service providers shall be liable to a party for any act or omission in connection with any administrative proceeding under this SDRP or the corresponding Rules. The complainant shall be directly and solely liable to the registrant in the event the complaint is granted in circumstances where the registrant is lawfully entitled to registration and use of the registered domain name(s) in the TLD.

8. Relation To Other Dispute Resolution Policies

This SDRP is in addition to and complementary with the Uniform Domain Name Dispute Resolution Policy ("UDRP"), the Uniform Rapid Suspension System ("URS") and any charter, nexus, or eligibility dispute policies adopted by ICANN or the Registry.

9. Effect of Other Proceedings

The administrative proceeding under the SDRP shall not prevent either party from submitting a dispute concerning the registered domain name in the TLD to concurrent administrative proceedings or to a court of competent jurisdiction for independent resolution during a pending SDRP administrative proceeding or after such proceeding is concluded. Upon notice of such other proceeding, the SDRP proceeding may be terminated (in the sole discretion of the Panelist) in deference to the outcome of such other proceeding.

10. SDRP Modifications

The FORUM reserves the right to modify this SDRP at any time subject to the terms of its MoU with the Registry. Such revised SDRP shall be posted on the FORUM Website at least thirty (30) calendar days before it becomes effective;[5] unless this SDRP has already been invoked by the submission of a complaint, in which event the version of the SDRP in effect at the time it was invoked will apply until the dispute is concluded. In the event that registrant objects to a change in this SDRP, the sole remedy is to cancel the registration, provided that registrant will not be entitled to a refund of any fees paid in connection with such registration.

[5] The FORUM may correct typographical errors without notice.

Naming Policy

Naming Policy

This Naming Policy sets forth the rules and guidelines concerning the availability of any domain name registered in this TLD. Here are the most current version of this Naming Policy and related material, including lists of Reserved Names, Blocked Names, and names that are blocked by ICANN. Certain other reserved and blocked names are provided exclusively to accredited Registrars.

This Naming Policy is part of the Registry Policies, which form a cohesive framework and must be read in conjunction with one another, as well as with other applicable agreements, policies, laws, and regulations which, taken together, represent the entirety the obligations and responsibilities with regard to any domain name registration.

Actual or attempted registration of a domain name in contravention of this Naming Policy may result in a Registrant being forbidden from registering domain names and/or the suspension or revocation of such Registrant's right to continue to be recognized as the Registrant of the non-compliant domain name or any other domain name. Suspension or revocation may, as determined in the Registry's sole discretion, with the cooperation of the sponsoring Registrar, apply to one or more of the Registrant's domain names.

The Registry reserves the right to modify or update this Naming Policy at any time and from time to time, and any such modifications or updates shall be posted on the Registry website. Once posted, such modified or updated Naming Policy shall apply to all Registrants.

1. Reserved Names

Reserved names may be reserved by ICANN or the Registry.

a. Reserved Names:

i. ICANN Reserved Names:

A. IGO/NGO Names

B. Country and Territory Names

ii. Names Reserved by the Registry:

A. Some domain names are reserved by the Registry for use in its operations.

b. In the event that a Registrant has mistakenly been allowed to register a Reserved Name, the Registry will, in its sole discretion, with the cooperation of the sponsoring Registrar, cancel or transfer such domain name. Any fees paid by the Registrar to the Registry will be refunded but the Registrant and the Registrar shall have no further recourse under the Registry Policies or otherwise.

c. In the event that a Registrant has fraudulently obtained the registration of a Reserved Name, the Registry reserves the right to cancel or transfer such domain name registration as provided for in, and take such further action as authorized by, the Registry Policies.

d. Registrants are not allowed to register a domain name that might be considered confusingly similar to a reserved name. In the event that Registry determines, in its sole and absolute discretion, that a domain name is confusingly similar to a reserved name, the Registry reserves the right to cancel or transfer such domain name registration as provided for in, and take such further action as authorized by, the Registry Policies.

2. Blocked Names

The Registry reserves the right, in its sole discretion, to block certain names and terms from registration. The Registry may also block certain Domain Names in accordance with applicable law or ICANN Consensus Policies. In the event the Registry has mistakenly allowed the registration of a Blocked Name, the Registry may, after refunding fees to the Registrar, transfer the name back to the blocked list.

3. Infringing Domain Names

Registrants are not allowed to register domain names that include terms that infringe upon intellectual property or other rights. More extensive discussions of infringement and the rights and responsibilities of both the rights holder and the alleged infringer can be found at ICANN's discussion of the UDRP, URS, and the TMCH claims service.

a. Terms that may infringe upon the rights of others include, but are not limited to:

   i. company names, brand names, or product names;

   ii. sport team and association names;

   iii. terms that may mislead the public as to a connection with or the source of goods or services, or the true identity of a person.

iv. names that falsely misrepresent themselves as a government entity, associated with the government, or approved by the government

b. Registration or use of a domain name may be infringing if:

i. the domain name is identical or confusingly similar to a personal name, company, business, or other legal or trade name, or to a trade or service mark in which a third party has uncontested rights, including without limitation in circumstances which:

1) the registration or use is likely to deceive or confuse others in relation to the source of goods or services provided under or in relation to, or in respect of similar goods or closely-related services of a registered trademark; or

2) the registration or use deceives or confuses others in relation to the source of goods or services in respect of which an unregistered trademark or service mark has become a distinctive identifier of the goods or services of a third-party complainant and in which the third-party complainant has established a legal right; or

3) the registration or use trades on or passes off a domain name or a website or other content or services access through a resolution of a domain name as being the same as or endorsed by, authorized by, associated with, or affiliated with the established business, name, or reputation of another; or

4) the registration or use constitutes intentionally misleading or deceptive conduct in breach of the Registry Policies, applicable laws, or ICANN Consensus Policies; or

5) the domain name has been registered or used in bad faith, which includes, without limitation, the following:

A. the Registrant has registered or used the domain name primarily for the purpose of unlawfully disrupting the business or activities of another person or entity; or

B. by registering or using the domain name, the Registrant has intentionally created a likelihood of confusion with respect to the third-party complainant's intellectual property rights or rights of publicity and as to the source, sponsorship, affiliation, or endorsement of website(s), email, or other online locations

or services of a product or service available on or through resolution of the domain name.

c. The Registry does not reserve or block domain name registrations for terms, or confusingly similar terms, that might infringe upon intellectual property or other rights. It is the responsibility of the Registrant to determine, prior to registering a domain name, whether or not a term might infringe the intellectual property or other rights of an entity or individual. The Registrant is solely liable in the event that the Registrants' use of a domain name constitutes an infringement or other violation of a third party's intellectual property or other rights.

d. In the event that any party disputes a Registrant's legal right to register and/or use a domain name that allegedly infringes the rights of another or that allegedly infringing material is displayed on a website that is resolved via the domain name, the Registrant shall act in accordance with and agrees to be bound by ICANN's policies, including the UDRP and URS, and by the Registry Policies, as applicable.

e. In the event that a Registrant has registered a domain name that infringes the rights of another, the Registry reserves the right, in cooperation with the sponsoring Registrar, to cancel or transfer such domain name registration as provided for in, and take such further action against Registrant as authorized by, these Registry Policies.

4. Other Naming Policies

a. Prospective Registrants are not permitted to submit an application for a domain name if they have previously submitted an application for registration for the same domain name where:

   i. they are relying on the same eligibility criteria for each domain name applications; and

   ii. the character string has previously been rejected by the Registry.

b. Registrants who repeatedly try to register Reserved Names, Blocked Names, or domain names that infringe the rights of others may be banned from further registration of domain names and may have any domain names registered to them revoked or cancelled, as provided for in the Registry Policies.

Acceptable Use Policy

Acceptable Use Policy

This Acceptable Use Policy (AUP) sets forth the terms and conditions for the use by a Registrant of any domain name registered in the top-level domain (TLD).

This Acceptable Use Policy (AUP) is part of the Registry Policies, which form a cohesive framework and must be read in conjunction with one another, as well as with other applicable agreements, policies, laws, and regulations which, taken together, represent the entirety the obligations and responsibilities with regard to any domain name registration.

The current version of the AUP will made available on the Registry website. It applies to any domain name registered in the TLD, no matter when or how registered, renewed, or transferred. Where a Registrant licenses or leases the domain name or any sub-domain names obtained under these Registry Policies, the Registry and the sponsoring Registrar shall hold the Registrant solely liable for activity in the domain name and, if applicable, in any sub-domain.

The Registry supports the free flow of information and ideas over the internet. The Registry does not and cannot exercise editorial control over the content of any message or web site made accessible by domain name resolution services in the TLD.

The Registry, with the cooperation of the sponsoring Registrar, may suspend, revoke, transfer, or modify the information or services provided in relation to any domain name (for example, through modification of a Registry Zone File) to address alleged violations of this AUP (described further below). The Registry shall have the authority to determine, in its sole discretion, whether use of a domain name is a prima facie violation of this AUP. The Registry or affected third parties may also utilize ICANN-sanctioned procedures, such as the Uniform Domain Name Dispute Resolution Policy (UDRP) or the Uniform Rapid Suspension (URS) system and/or applicable courts (including those courts in the jurisdiction and venue specified in the Registrant Agreement).

Registrants are obliged and required to ensure that their use of a domain name is at all times lawful and in accordance with the requirements of the Registry Polices and applicable laws and regulations, including those of the Registrant's country of residence and ICANN Consensus Policies - including but not limited to those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, disclosure of data, and financial disclosures. Registrants who collect and maintain sensitive health and financial data must implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law. Where applicable, Registrants represent that they

possess any necessary authorizations, charters, licenses and/or other related credentials for participation in the sector associated with the TLD; material changes to the validity of such credentials must be reported to the Registry.

The Registry reserves the right to modify or amend this AUP at any time and from time to time and any such updates shall be posted on the Registry's website. The Registry will notify Registrars in the event of updates. The AUP as posted on the Registry's website is the agreement in affect at any time.

Prohibited Use

A Prohibited Use of a domain name is a use that is either illegal or expressly prohibited by provisions of this AUP and/or the Registry Policies. A non-exhaustive list of such restrictions pertaining to registration or use of a domain name (in relation to various purposes and activities) is further described below in this AUP.

Compliance with the Registry's AUP

The registration and use of a domain name in the TLD must be for lawful purposes. The creation, transmission, distribution, storage of, or automatic forwarding to or framing of any material in violation of applicable laws, regulations, or this AUP is prohibited. This may include, but is not limited to, the following:

a. Communication, publication, or distribution of material (including through forwarding or framing) that infringes the intellectual property rights and/or right of publicity of another person or entity. Intellectual property rights include, but are not limited to: copyrights, design rights, patents, patent applications, trademarks, rights of personality, rights of publicity and trade secret information. Rights of publicity include, but are not limited to, the right to keep one's image and likeness from being commercially exploited without permission or contractual compensation, the right to be left alone, and the right to be forgotten.

b. Cyber bullying or other harassment.

c. Registration or use of a domain name that, in the sole discretion of the Registry violates the Naming Policy.

d. Registration or use of a domain name that is part of a pattern of registration or use where the Registrant has registered or used domain names that violate the Naming Policy;

e. Failure of the Registrant to transfer the domain name to a third party if, as evidenced in writing, Registrant acted as an agent of the third party when registering for the domain name.

f. Use of content or methods that, in the sole discretion of the Registry:

   i. are capable of disruption of systems in use by other internet users or service providers (e.g., viruses or malware);

   ii. seek or apparently seek authentication or login details used by operators of other internet sites (e.g., phishing); or

   iii. may mislead or deceive visitors to the site that the site has an affiliation with the operator of another internet site or business (e.g., phishing); or

g. Use of the domain name to publish or distribute, either directly or through forwarding or framing, images or materials that are prohibited by or constitute an offense under applicable laws, including the law of the Registrant's country of residence.

h. Use of the domain name to publish or distribute material that includes, by way of example and without limitation, real or manipulated images depicting the sexual exploitation of children, bestiality, and material containing threats or detailed instructions regarding how to commit a crime.

i. Use of the domain name to publish or distribute defamatory material or material that constitutes racial vilification or "hate speech."

j. Use of the domain name to publish or distribute material that constitutes an illegal threat or encourages conduct that may constitute a criminal act.

k. Use of the domain name to publish or distribute material that is in contempt an order of a court or other authoritative government actor within the jurisdiction of the country of residence of the Registrant, Registrar, or Registry.

Electronic Mail

The Registry expressly prohibits Registrants from engaging in the following activities:

a. Communicating, transmitting, or sending unsolicited bulk email messages or other electronic communications ("junk mail" or "spam") of any kind including, but not limited to, unsolicited commercial advertising and informational announcements as prohibited by applicable law.

b. Communicating, transmitting, or sending any material by email or otherwise that harasses another person or that threatens or encourages bodily harm or destruction of property.

c. Communicating, transmitting, sending, creating, or forwarding fraudulent offers.

Disruption of the Registry Network

A Registrant may not use a domain name for the purpose of:

a. Restricting or inhibiting any person in their use or enjoyment of the Registry's network or a domain name or any service or product of the Registry.

b. Actually, or purportedly reselling the Registry's services or products without the prior written consent of the Registry.

c. Communicating, transmitting, or sending very large or numerous pieces of email or illegitimate service requests (i.e., a DDoS attack).

d. Providing false or misleading information to the Registry.

e. Facilitating or aiding the transmission of confidential information, private, personal or stolen data including, but not limited to, credit card information (without the owner's or cardholder's express prior written consent).

Network Integrity and Security

a. Registrants are prohibited from circumventing or attempting to circumvent the security of any host, network, or accounts (i.e., cracking or hacking) on, related to, or accessed through the Registry's network. This includes, but is not limited to:

    i. accessing data not intended for the Registrant;

    ii. logging into a server or account which the Registrant is not expressly authorized to access;

iii. using, attempting to use, or attempting to ascertain a username or password without the express written consent of the operator of the service in relation to which the username or password is intended to function;

iv. probing the security of other networks; and/or

v. executing any form of network monitoring that is likely to intercept data, of any nature, not intended for the Registrant.

b. Registrants are prohibited from effecting any network security breach or disruption of any internet communications including, but not limited to:

i. accessing data of which the Registrant is not an intended recipient; and/or

ii. logging onto a server or account which the Registrant is not expressly authorized to access.

For the purposes of this section, "disruption" includes, but is not limited to:

+ port scans, TCP/UDP floods, packet spoofing;

+ forged routing information;

+ deliberate attempts to overload or disrupt a service or host; and/or,

+ using the Registry's network in connection with the use of any program, script, command, or sending messages with the intention or likelihood of interfering with another user's terminal session by any means, locally or by the internet.

c. Registrants who compromise or disrupt the Registry's network systems or security may incur criminal or civil liability. The Registry will investigate any such incidents and will notify and cooperate with law enforcement and other appropriate governmental actors if an alleged crime or other alleged wrongdoing in violation of this AUP is suspected to have taken place.

Non-Exclusive, Non-Exhaustive

This AUP is intended to provide guidance as to acceptable use of the Registry's network and domain names. However, the AUP is neither exhaustive nor exclusive.

Enforcement

The Registry may, in its sole discretion, with the cooperation of the sponsoring Registrar, suspend, transfer, or terminate a Registrant's service, including a domain name registration, for violation of any of the terms and conditions of the AUP on receipt of a complaint if the Registry, in its sole discretion, believes:

a. a violation of the AUP has or may have occurred; and/or

b. suspension and/or termination may be in the public interest.

Except in extreme situations, the Registry may work with Registrars to effect the appropriate action.

Complaints regarding violations of this policy or law should be directed to the Abuse Point of Contact at abuse@mmx.co or by mail to Minds + Machines Group Limited office at 32 Nassau Street, Dublin 2, Ireland.

DISCLAIMER AND LIMITATION OF LIABILITY

THE REGISTRANT ACKNOWLEDGES AND AGREES THAT, TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE REGISTRY AND THE REGISTRY RELATED PARTIES SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF PROGRAMS OR OTHER DATA, OR OTHERWISE RELATING TO THE USE, SUSPENSION, TERMINATION OR THE INABILITY TO USE THE DOMAIN NAME OR IN ANY OTHER WAY RELATED TO THE DOMAIN NAME, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING IN THE CASE OF NEGLIGENCE BY THE REGISTRY AND/OR REGISTRY RELATED PARTIES), OR OTHERWISE. THE REGISTRY'S LIABILITY FOR ANY BREACH OF A CONDITION OR WARRANTY IMPLIED BY ANY OF THE REGISTRY POLICIES, INCLUDING THE LAUNCH PHASE POLICIES, THE SUNRISE DISPUTE RESOLUTION POLICY, NAMING POLICY, ACCEPTABLE USE POLICY, COMPLAINT RESOLUTION SERVICE POLICY, PRIVACY POLICY, REGISTRANT AGREEMENT, AND/OR THE REGISTRY–REGISTRAR AGREEMENT SHALL BE LIMITED TO THE MAXIMUM EXTENT POSSIBLE TO ONE OF THE FOLLOWING (AS THE REGISTRY MAY DETERMINE IN ITS SOLE DISCRETION:

A. SUPPLYING THE DOMAIN NAME AGAIN; OR

B. PAYING THE REASONABLE COST INCURRED OF HAVING THE SERVICES SUPPLIED AGAIN.

ADDITIONALLY, TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE REGISTRY AND THE REGISTRY RELATED PARTIES SHALL NOT BE LIABLE FOR ANY LOSSES OR DAMAGES THAT THE REGISTRANT MAY INCUR AS A RESULT OF UNAUTHORIZED USE OF THE DOMAIN ARISING FROM "HACKING," DENIAL OF SERVICE ATTACK, VIRUS, WORM, OR OTHERWISE, OR FOR LACK OF FITNESS FOR A PARTICULAR PURPOSE OF THE DOMAIN NAME OR SERVICES RELATED TO THE DOMAIN NAME.

IN THE EVENT THAT THE REGISTRY OR A REGISTRY RELATED PARTY TAKES ACTION WITH RESPECT TO A REGISTRY DOMAIN NAME PURSUANT TO THE REGISTRY POLICIES, WHICH ACTION IS REVERSED, MODIFIED, OR ACKNOWLEDGED TO HAVE BEEN INCORRECT BY THE REGISTRY AND/OR A REGISTRY RELATED PARTY OR BY A COURT OF FINAL DETERMINATION, THEN REGISTRANT AGREES THAT, TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE REGISTRY AND/OR REGISTRY RELATED PARTIES SHALL NOT BE LIABLE FOR ANY DAMAGES THAT THE REGISTRANT MAY SUFFER THEREBY, EVEN IF THE REGISTRY AND/OR REGISTRY RELATED PARTIES HAVE BEEN ADVISED OF THE POTENTIAL FOR SUCH DAMAGES, AND EVEN IF THE REGISTRY AND/OR REGISTRY RELATED PARTIES MAY FORESEE SUCH POSSIBLE DAMAGES. THE REGISTRANT'S SOLE REMEDY UNDER SUCH CIRCUMSTANCES SHALL BE THE RESUPPLY OF THE DOMAIN NAME OR, AT THE SOLE DISCRETION OF THE REGISTRY, A REFUND OF THE REGISTRATION FEE, SUNRISE FEE, RENEWAL FEE (IF THE CIRCUMSTANCE OCCURRED DURING A RENEWAL TERM) OR REDEMPTION FEE, WHICH REMEDY THE REGISTRANT AGREES CONSTITUTES THE ONLY POSSIBLE DIRECT DAMAGES FLOWING FROM THIS AGREEMENT.

IN ADDITION, THE REGISTRY AND/OR REGISTRY RELATED PARTIES ARE, TO THE MAXIMUM EXTENT PERMITTED BY LAW, NOT LIABLE FOR ANY DAMAGES THAT THE REGISTRANT MAY SUFFER BECAUSE OF SERVICE OR SYSTEM FAILURE, INCLUDING DOMAIN NAME SYSTEM FAILURE, ROOT SERVER FAILURE, TELECOMMUNICATION FAILURE, INTERNET PROTOCOL ADDRESS FAILURE, ACCESS DELAYS OR INTERRUPTIONS, DATA NON-DELIVERY OR MIS-DELIVERY, ACTS OF GOD, UNAUTHORIZED USE OF PASSWORDS, ERRORS, OMISSIONS OR MIS-STATEMENTS IN ANY INFORMATION OR OTHER SERVICES PROVIDED UNDER THIS AGREEMENT, DELAYS OR INTERRUPTIONS IN DEVELOPMENT OF WEB SITES, RE-DELEGATION OF THE REGISTRY TOP-LEVEL DOMAIN NAME, OR BREACH OF SECURITY, EVEN IF THE REGISTRY AND/OR REGISTRY RELATED PARTIES HAVE BEEN ADVISED OF THE POTENTIAL FOR SUCH DAMAGES, AND EVEN IF THE REGISTRY OR REGISTRY RELATED PARTIES MAY FORESEE SUCH POSSIBLE DAMAGES. THE REGISTRANT'S SOLE REMEDY FOR THE REGISTRY OR REGISTRY RELATED PARTIES' BREACH OF THIS AGREEMENT OR NEGLIGENCE OF ANY TIME SHALL BE, AT THE SOLE DISCRETION

OF THE REGISTRY OR THE REGISTRY RELATED PARTIES, THE RESUPPLY OF THE DOMAIN NAME OR A REFUND OF THE REGISTRATION FEE, REDEMPTION FEE OR RENEWAL FEE (IF THE BREACH OCCURS DURING A RENEWAL TERM), WHICH REMEDY THE REGISTRANT AGREES CONSTITUTES THE ONLY POSSIBLE DIRECT DAMAGES FLOWING FROM THIS AGREEMENT. THE REGISTRANT'S SOLE REMEDY FOR AN ACTION NOT FLOWING FROM THIS AGREEMENT (IN TORT OR OTHERWISE) SHALL BE LIMITED TO THE AMOUNT OF MONEY PAID TO THE REGISTRY OR REGISTRY RELATED PARTIES BY THE REGISTRANT.

Modification of Network Data

The Registry is committed to an open internet and to freedom of expression. However, in the course of its duties to comply with ICANN consensus policies, UDRP, or URS decisions, court or other governmental orders, or other duly-qualified law enforcement requests, or to protect the integrity and functioning of its networks, the Registry, in its sole discretion, reserves the right to:

a. remove or alter content, Zone File data and/or other material from its servers that violates the provisions or requirements of this AUP;

b. re-delegate, redirect or otherwise divert traffic intended for any service;

c. notify operators of internet security monitoring services, virus scanning services and/or law enforcement authorities of any breach or apparent breach of this AUP or other Registry Policies; and/or

d. terminate access to the Registry's network by any person or entity that the Registry determines has violated the provisions or requirements of this AUP.

Complaint Resolution Service

Complaint Resolution Service

This Complain Resolution Service (CRS) is part of the Registry Policies, which form a cohesive framework and must be read in conjunction with one another, as well as with other applicable agreements, policies, laws, and regulations which, taken together, represent the entirety the obligations and responsibilities with regard to any domain name registration.

Ordinarily, the Registry is unable to simply suspend a domain name where another member of the public complains or takes issue with the use to which a domain name is being put and a concerned member of the public always has the right to reach out to the domain name Registrant directly to bring any concerns to their attention.

If such direct contact is not possible or advisible (it may be a sensitive concern after all), or if after doing so, there is still a concern that the registration or use of a domain name in the TLD is illegal, abusive, infringes the rights of others, is otherwise in violation of the Registry Policies, or is allegedly otherwise in violation of the law, we provide the CRS, through which anyone may register a complaint.

The CRS provides a transparent, efficient, and cost effective way for the public, including law enforcement, regulatory bodies, and intellectual property owners to (a) submit complaints or report concerns regarding the registration or use of a domain name in the TLD, and (b) where appropriate, to seek to have such concerns addressed through confidential and non–binding mediation.

Managed through the Abuse Point of Contact, the CRS provides a procedure for reporting and, where appropriate, addressing alleged illegal or prohibited conduct effected through a domain name in the TLD; prohibited conduct includes, but is not limited to: inaccurate Registrant Whois information; that a domain name registration is being used to facilitate or promote malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting, or activity otherwise contrary to applicable law. The CRS framework employs two levels of review: (1) immediate action to protect the public interest, or (2) the optional appointment of an independent Ombudsperson to facilitate, where possible, confidential and non-binding complaint resolution between the parties.

The CRS is not intended to replace courts or ICANN-mandatory dispute resolution systems such as the UDRP (Uniform Domain Name Dispute Resolution Procedure) or URS (Uniform Rapid Suspension system).

Complaints and reports of concern will be reviewed as follows:

Step One: Confirmation and Communication

The Abuse Point of Contact will initially review all complaints and reports of concerns regarding alleged criminal or otherwise illegal or prohibited conduct for compliance with the Registry Policies.

Upon receipt of any Complaint, the Abuse Point of Contact will "lock" the domain name and associated records until the Complaint is determined frivolous, resolved, withdrawn, or dismissed, or pursuant to a court order or reasonable request from law enforcement. A Complaint shall not exceed 1,000 words or three (3) pages, whichever is less.

Review Tier 1: immediate action to protect the public interest: In the event of a report of alleged criminal or otherwise illegal or prohibited conduct requiring immediate action to protect the public interest, the Abuse Point of Contact will initiate an "Immediate Review of Request for Suspension in the Public Interest" (see Step Two below).

Review Tier 2: optional appointment of an independent Ombudsperson: In the event of a Complaint alleging non-compliance with the Registry Policies that does not require immediate action to protect the public interest, the Abuse Point of Contact will contact the parties to explore their interest in confidential and non-binding mediation aimed at facilitating an amicable resolution between the parties (see Steps Three through Seven below).

If the Abuse Point of Contact considers that the Complaint does not address a matter covered by the Registry Policies, is deficient, or is frivolous, the filing/complaining party (Complainant) will be promptly notified of the deficiencies identified. The Complainant has five (5) business days from the receipt of notification to correct the deficiencies and return the Complaint, failing which, the Abuse Point of Contact will deem the Complaint to be withdrawn and the domain lock will be removed. This will not prevent the Complainant from submitting a different Complaint in the future.

Step Two: Immediate Review of Request for Suspension in the Public Interest

On receipt of a Complaint or report of alleged criminal or otherwise illegal or prohibited conduct requiring immediate action to protect the public interest, the Abuse Point of Contact will initiate an "Immediate Review of Request for Suspension in the Public Interest" to determine, whether or not specifically requested by the Complainant, if a Critical Issue Suspension (CIS) is warranted.

A request for a CIS may be granted in cases where there is a compelling and demonstrable threat to the stability of the Internet, critical infrastructure, or

public safety. A CIS does not terminate the Registrant's rights or their domain name registration; it simply modifies the Name Server records in the zone, temporarily disabling resolution. Suspensions under the CRS, including a CIS, may be appealed to the Ombudsperson's office for resolution.

Absent compelling circumstances including, but not limited to, a court order or reasonable request from law enforcement, where the Abuse Point of Contact has activated a CIS, a suspension notice will be sent to the Registrant's administrative contact with a copy to the Registrar, usually within 48 hours.

Step Three: Formal Notification of Complaint

Any Complaint alleging non-compliance with the Registry Policies must be submitted to the Abuse Point of Contact provided on the Regsitry's website; all required information must be complete, the Complaint must be signed electronically, and any fee required must be paid in advance of the Abuse Point of Contact attending to the complaint. The types of conduct that may be raised as the basis for a Complaint alleging non-compliance with the Acceptable Use Policy can be found on the Registry's website.

In the event that a Complaint alleging non-compliance with the Registry Policies is submitted to the Abuse Point of Contact, typically within 5 business days of receipt of the Complaint, the Abuse Point of Contact will send a "Formal Notification of Complaint" including a copy of the Complaint, by email to the Respondent using the administrative contact details provided in the Whois for the domain name as well as to any other Registrant email addresses provided by the Complainant.

Either Party may provide an additional email address by notifying the Abuse Point of Contact; the Registrant may not, however, change the Registrant information for the domain name without mutual agreement of the parties or unless a settlement is reached.

Communications must be in English and any email attachments should be in a standard format, such as Microsoft Word or PDF, and should not exceed 10MB individually or 50MB together.

Any communication between the Parties shall copy the other Party, the Abuse Point of Contact, and the Ombudsperson, if appointed.

Except as otherwise decided by the Abuse Point of Contact in its sole discretion, all communications under the CRS shall be deemed received at the date and time on which the email or communication was sent as determined by the time

zone of the Abuse Point of Contact; in case of doubt, however, it shall be the responsibility of the sending party to provide proof of transmission.

Step Four: Commencement of Complaint Resolution Service Proceedings

At the same time as the notification to the Parties (by email) of the commencement of a CRS proceeding, the Abuse Point of Contact will contact the parties to explain the confidential and non-binding nature of the CRS, and to gauge their interest in Registry-facilitated mediation aimed at allowing the Parties to reach an amicable solution.

For the avoidance of doubt, even if the Parties do not decide to engage in CRS-based mediation, the Registry may, in its sole discretion (including based on reports made to the Registry by third parties), suspend, transfer, or terminate a Registrant's service, including a domain name registration, for violation of any of the requirements or provisions of the Registry Policies on receipt of a complaint if the Registry believes (a) a violation has or may have occurred; and/or (b) suspension and/or termination may be in the public interest. Also, for the avoidance of any doubt, the Respondent may submit a Response even if it decides not to participate in mediation, e.g., to provide information to the Registry as to any alleged non- compliance.

Step Five: the Response

Within fifteen (15) business days of the date of commencement of a CRS proceeding, the Respondent (i.e., the domain name Registrant) may submit a Response. The Response must be submitted to the Abuse Point of Contact provided on the Registry's website; all required information must be completed, and the Response must be signed electronically.

The Response shall:

1. specifically dispute each alleged instance of non-compliance (the "grounds for the Complaint") raised by the Complainant that the Respondent wishes to rely upon to rebut the Complainant's assertions;
2. indicate whether the Respondent wishes to be contacted directly or through an authorized representative—if the Respondent wishes to use an authorized representative, their contact details including email address must be provided;
3. mention whether any legal proceedings have been commenced (even if terminated) in connection with the domain name(s) which is the subject of the Complaint; and
4. notexceed1,000words or three(3)pages, whichever is less.

Once submitted, a copy of the Response will be forwarded to the Complainant and to the Respondent as soon as practicable. In the event there is no Response, the Complaint shall be deemed closed; the Parties may however submit a new Complaint in future, or a UDRP or URS or court claim.

Step Six: Reply by the Complainant

Within five (5) business days of receiving the Respondent's Response, the Complainant may submit a Reply to the Respondent's Response, which shall not exceed 1,000 words or three (3) pages, whichever is less (annexes may only be included with the permission of the Abuse Point of Contact). The Reply should be confined to answering any new points raised in the Response that could not have reasonably been foreseen when the Complaint was submitted.

Step Seven: Amicable Complaint Resolution (Ombudsperson)

Complaint Resolution Service

If the Parties have agreed to mediation, within ten (10) business days of the receipt of the Complainant's Reply (or the expiry of the deadline to do so), the Abuse Point of Contact will arrange with the Ombudsperson's office for mediation to be conducted. Mediation will be conducted in a manner that the Ombudsperson, at their sole discretion, considers appropriate.

Mediation conducted between the Parties during mediation (including any information obtained from or in connection to negotiations) shall be strictly confidential as between the Parties and the Ombudsperson. Neither the Ombudsperson nor any Party may use or reveal details of such negotiations to any third parties (including a UDRP or URS provider) unless ordered to do so by a court of competent jurisdiction.

If the Parties reach settlement during the mediation, then the existence, nature, and terms of the settlement shall be confidential as between the Parties unless the Parties specifically agree otherwise, a court competent jurisdiction orders otherwise, or applicable laws or regulations require it.

Any settlement reached by the Parties must be in writing to be enforceable and should include instructions for the Registry (and if applicable, Registrar) concerning the disposition of domain name and timing; the Ombudsperson will provide a (non-mandatory) template for such purposes.

If the Parties did not achieve an acceptable resolution through mediation within twenty (20) business days of the appointment of an Ombudsperson, the Ombudsperson will send notice to the Parties and Abuse Point of Contact that it

does not appear that the Complaint can be resolved through the CRS. In such case, the Complainant shall have the option of availing itself of the courts or other processes such as the UDRP or URS. The Registry shall unlock the domain name within fifteen (15) business days of such notice from the Ombudsperson.

Effect of Court Proceedings

If, before or during the course of proceedings under the CRS, the Ombudsperson or Abuse Point of Contact is made aware that legal proceedings have begun in or before a court or other body of competent jurisdiction, including but not limited to a URS or UDRP proceeding, and that such legal proceeding specifically relates to a domain name and conduct which is the subject of a Complaint, the CRS will be terminated.

A Party must promptly notify the Ombudsperson if it initiates or becomes aware of legal proceedings before a court or panel of competent jurisdiction, including but not limited to a URS or UDRP proceeding, relating to a domain name which is the subject of a Complaint during the course of proceedings under the CRS.

The applicable fees with respect to the referral of proceedings under the CRS to the Ombudsperson are (in Euros) €50 plus applicable taxes for Complaints involving 1-5 domain names and only one Complainant. For Complaints involving 6 or more domain names, the Ombudsperson and/or Abuse Point of Contact will set a fee in consultation with the Abuse Point of Contact. Fees are calculated on a cost-recovery basis; the Registry does not intend profit from its mediation or administration services of the Complaint Resolution Service.

Exclusion of Liability

Neither the Registry employees, directors, officers, representatives, delegees, shareholders, agents, successors, and/or assigns or those of its affiliates; nor any employee or agent of the Ombudsperson shall be liable to a Party for anything done or omitted, whether (to the extent permitted by applicable law) negligently or otherwise, in connection with any proceedings under the CRS unless the act or omission is shown to have been intentionally done in bad faith.

Privacy Policy

Privacy Policy

Minds + Machines Group Limited ("MMX") is committed to the privacy of its customers and users of the mmx.co website (the "Site") and any services that may be offered by MMX on the Site. The Site is owned by MMX, and operated on its behalf by Minds + Machines Limited, 32 Nassau Street, Dublin 2, Ireland, Co. No. 516026. We take our responsibilities under the Data Protection Acts, 1988 and 2003, seriously, and we are committed to protecting your privacy when you are using our online and other services. This privacy policy governs the manner in which we use, maintain and disclose information collected from customers as well as users of the Site.

Controller, contact, data protection officer

Controller pursuant to Art. 4 (7) EU General Data Protection Regulation ("GDPR") is

Minds + Machines Limited
32 Nassau Street
Dublin 2
Republic of Ireland

In case of questions or comments concerning this privacy policy, please contact our data protection officer by e-mail at privacy@mmx.co or by post at

Data protection officer
c/o Minds + Machines Limited
32 Nassau Street
Dublin 2
Republic of Ireland

How MMX Uses Personal Data

MMX may use information provided by you:

- To process your request to become a registrar.
- To ensure that content from our site is presented in the most effective manner for you and for your computer.
- To provide you with information, products, or services that you request from us or which we believe may interest you, where you have consented to be contacted for such purposes.
- To carry out our obligations arising from any services we are contracted to provide you.
- Additionally, MMX may also use personal data to improve the level and type of services offered to customers, such as processing personal data for the purposes of sales analysis and customer usage statistics; to improve the content, design, and layout of the mmx.co website; to facilitate

knowledge management; and to understand the interests and buying behavior of our registered users.

- We may monitor and record our communications with you, including emails and telephone conversations. Information collected may then be used for training purposes, quality assurance, to record details about products/services in which you are interested, and in order to meet our legal obligations in general. Please note the information below regarding the use of third-party cookies.

If you do not want us to use your data in this way, or to pass your details on to third parties for marketing purposes, please contact us as provided for below.

Legal bases for processing of your data

Unless specifically stated, the following legal bases apply to the processes listed below:

- Insofar as we obtain the data subject's consent for processing, Art. 6 (1) Clause 1 lit. a) GDPR is the legal basis.
- In case of processing of personal data necessary for the fulfillment of a contract, the legal basis is Art. 6 (1) Clause 1 lit. b) GDPR.
- Insofar as processing of personal data is necessary for the fulfillment of a legal obligation, the legal basis is Art. 6 (1) Clause 1 lit. c) GDPR.
- In the event that vital interests of the data subject or of another natural person require a processing of personal data, the legal basis is Art. 6 (1) Clause 1 lit. d) GDPR.
- If processing is necessary to safeguard legitimate interests of our company or of a third party and if the interests, basic rights, and basic freedoms of the data subject do not outweigh these legitimate interests, the legal basis for processing is Art. 6 (1) Clause 1 lit. f) GDPR.

Retention periods

The data processed by us is erased or its processing is restricted in compliance with statutory requirements, in particular Art. 17 and 18 GDPR. Unless expressly stated otherwise within the scope of this privacy policy, we erase data stored by us as soon as such is no longer required for the intended purpose. Data will be retained beyond the time at which the purpose ends only if such data is necessary for other legally permissible purposes or if the data must continue to be retained due to statutory retention periods. In these cases, processing is restricted, i.e. it is blocked, and will not be processed for other purposes.

Processors, Third Party Service Providers

In some cases, we use external service providers to process your data, which are bound to our instructions. They were selected and commissioned by us with care and they are monitored regularly. The orders are based on data processing agreements pursuant to Art. 28 GDPR. The processor does not independently process data for its own purposes. Further, they must process the personal information in accordance with this privacy notice and as permitted by applicable data protection laws.

The information that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). It may also be processed by staff operating outside the EEA who work for us or for one of our vendors. Such staff may be engaged in, among other things, the processing or fulfillment of services, and the provision of support services. By submitting your personal data you agree to this transfer, storing, or processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy and we will comply with the GDPR.
MMX will also actively investigate and cooperate with law enforcement agencies regarding any allegations of abuse or violation of system or network security or other laws.

Cookies

We use cookies. Cookies are small text files that within the scope of your visit of our website are transmitted from our web server to your browser and are stored by your browser on your computer for later retrieval. You yourself can determine, through settings in your browser, the extent to which cookies can be placed and retrieved. Persistent cookies may be stored on your computer after your visit and our website can access them every time each time you visit our website (so-called "ID cookies"). Some cookies that are stored during your visit of our website can be stored and retrieved by other companies.

Legal basis for the use of cookies is Art. 6 (1) Clause 1 lit. a), lit. f) GDPR unless specified otherwise.

The following types of cookies can be set on your device:

- Strictly necessary cookies: These cookies enable services you have specifically asked for, e.g. identifying you as being signed in with the Site user ID and password, and keeping you logged in throughout your visit. These cookies do not contain any personally-identifiable information and are typically set by MMX.
- Performance cookies: These cookies are used to collect statistical information about visitors to the Site and the pages they view. These

cookies do not collect information that identifies a visitor, and all information is aggregated and used anonymously. MMX use these cookies to understand what content is popular. For more information on how to manage cookies, including opt-out of performance cookies please visit: http://www.aboutcookies.org/Default.aspx?page=1

- Functional cookies: These cookies allow the Site to remember choices you make and provide enhanced and more personal features. MMX occasionally uses this type of cookie. Note that if you disable these cookies the Site may not work properly. For more information on how to manage cookies, including opting-out of functional cookies please visit http://www.aboutcookies.org/Default.aspx?page=1
- Targeting and advertising cookies: These cookies are used to deliver advertising that is more relevant to you and your interests. They are also used to limit the number of times you see an advertisement as well as help measure the effectiveness of the advertising campaign. For more information on how to manage cookies, including opting out of targeting and advertising cookies, please visit http://www.aboutcookies.org/Default.aspx
- Other third party cookies: Some cookies that have been set on our Site are not related to MMX. When you visit a page with content embedded from, for example, YouTube or a social network site, these service providers may set their own cookies on your web browser. We do not control the use of these cookies and cannot access them due to the way that cookies work. Cookies can only be accessed by the party that originally set them. You should check the third party websites for more information about these cookies.
- Other companies which advertise or offer their products or services on our website may also place cookies on your device. The types of cookies such other companies use and how they use the information generated by them will be governed by their respective privacy policies and not ours.

Log Files

For the informational use of the Site it is generally not required that you actively disclose your personal data. In this case we instead collect and use only the data automatically transmitted to us by your Internet browser. This includes:

- date and time of your retrieval of one of our websites;
- your browser type;
- your browser settings;
- utilized operating system;
- your most recently visited site;

- the transferred data volume and access status (file transferred, file not found, etc.);
- your IP address.

The data is stored on our servers. This data is not stored together with other personal data except those stated above. The temporary storage of the IP address by the system is necessary to allow delivery of the website to the user's computer. For this purpose, the IP address of the user must be stored for the duration of the session. We create so-called log files from this data. The created log files are stored to safeguard the security of our IT systems. A personal evaluation of the data, in particular for marketing purposes, does not take place.

Processing of the above data is required for technical reasons to offer a website pursuant to Art. 6 (1) Clause 1 lit. b), lit. c), lit. f) GDPR in order to correctly display our website to you and to safeguard stability and security. In particular, log files are created to verify attacks on our systems. We erase server log data from our systems regularly, at the latest every six months.

Newsletter

With your consent, you can subscribe to our newsletter in which we inform you of our current interesting offers. We use the so-called double opt-in process for registration to our newsletter. This means that after your registration, an email is sent to the disclosed email address, in which we ask you to confirm your request to receive the newsletter. We furthermore retain your utilized IP addresses and the time of registration and confirmation. The purpose of this process is to verify your registration and clarify a possible abuse of your personal data, if necessary. Only the disclosure of your email address is required to receive the newsletter. All other disclosed information is voluntary and will be used to allow us to address you personally. After your confirmation, we store your email address for sending you the newsletter. The legal basis for this is Art. 6 (1) Clause 1 lit. a) GDPR.

To unsubscribe from the newsletter, you can click on the link provided in every newsletter email or send an email to support@mmx.co. Newsletters are sent by the mail order service Sendgrid, 1801 California St., Suite 500, Denver, CO 80202, U.S.A. You can view Sendgrid's privacy policy at www.sendgrid.com/policies/privacy/ The legal basis for using Sendgrid is. Art. 6 para. 1 lit. f GDPR and a contract according to Art. 28 para. 3 p. 1 GDPR. Sendgrid is subject to the EU-US Privacy Shield, https://www.privacyshield.gov/EU-US-Framework

The newsletters contain "web beacons". These are pixel-sized files that are retrieved from a Sendgrid server when the newsletter is opened. Within this retrieval, technical information, such as data on the browser and your system, as well as your IP address and time of retrieval are initially processed.

This data is used to technically improve the services based on the technical data or the target groups and their reading behavior based on their retrieval locations (which can be determined using the IP address) or access times. The statistics also includes determining whether the newsletters are opened, when they are opened and which links are clicked. For technical reasons, this information can be assigned to the individual newsletter recipients. However, it is neither our intention, nor that of Sendgrid, to observe individual users. Therefore, statistical data will be anonymized as soon as possible. The evaluations serve us much more to recognize the reading habits of our users and to adapt our contents to them or to send different contents according to the interests of our users.

You can object to the analysis at any time by clicking on the separate link provided in each e-mail or by informing us of another contact method. The information is stored for as long as you have subscribed to the newsletter. After your opt-out we store the data purely statistically and anonymously.

Contacting

In case of contact by email or telephone, your data is processed, depending on the content of the request: for purely informational inquiries based on your (assumed) consent pursuant to Art. 6 (1) Clause 1 lit. a) GDPR; or pursuant to Art. 6 (1) Clause 1 lit. b) GDPR, insofar as contacting is connected to contractual performance obligations. In case of contacting through our online ticket submission system, we require only your email address in order to reply to you. Additionally, you can voluntarily disclose your name to allow us to address you personally. Your information may be stored in a customer relationship management system ("CRM system").

We delete your contact requests immediately after they are processed unless statutory retention periods require longer retention.

Service Announcements

On rare occasions it may be necessary to send out a strictly service-related announcement if, for instance, a service is temporarily suspended for maintenance. Generally, users may not opt-out of these communications. However, these communications are not promotional in nature. Legal basis for

processing is Art. 6 (1) lit. b) GDPR.

Legal Disclaimer

Though every effort is made to preserve your privacy, MMX may need to disclose personal information when required to by law, rule and/or regulation. MMX will comply with all such lawful requests should a court order, legal process, or similar be served on it.

This Site contains links to other websites. Please be aware that MMX is not responsible for the privacy practices or terms and conditions of such other websites. You are encouraged to read the privacy policies of each and every website that collects personally identifiable information. The MMX Privacy Policy as described herein applies solely to information collected by MMX.

Your Responsibilities

You are responsible for the security of your user ID(s) and password(s). Make sure you keep them in a safe place and do not share them with others.
Always remember to log out after your session ends, to ensure that others cannot access your private personal information. You should take this precaution even if you are not using a public computer, such as at a library or internet café, but also when using your private computer in your home.

Your Rights

Pursuant to statutory provisions, you can assert the following rights vis-à-vis the data processing controller free of charge:

- Right to access by the data subject (Art. 15 GDPR);
- Right to rectification and erasure (Art. 16 and Art. 17 GDPR);
- Right to restriction of processing (Art. 18 GDPR);
- Right to data portability (Art. 20 GDPR);
- Right to object (Art. 21 GDPR).

You also have the right to complain to a data protection supervisory authority concerning the controller's processing of your personal data.

Social media presences

We maintain presences in social media in order to communicate with customers and prospective customers there and to keep them informed. When utilizing the relevant social media network, the terms and conditions of the respective social

media network operators apply.

Data security

MMX takes the security and protection of your personal data very seriously. MMX utilizes appropriate internal security procedures that restrict access to and disclosure of personal data within MMX. We also apply technical and organizational security measures to protect personal data that is collected, in particular against accidental or intentional manipulation, loss, destruction or against the attack of unauthorized persons. Our security measures are continuously improved in line with industry standard technological developments.

Other Matters

Children: The Site is not intended for children and we ask that no-one under the age of 18 submit personal information to us or use the site without supervision of a parent or guardian.

Changes to this Policy: If we decide to change this privacy policy, we will post such changes on this page so that you are always aware of what information we collect, how we use it, and under what circumstances we disclose it, and where appropriate, notify you by email. Each time you access or use the site or services, you will be bound by the then-effective Privacy Policy.