Draft Accreditation & Access Model
For Non-Public Whois Data
March 27, 2018
Version 1.3

Introduction

To the ICANN Community, Privacy Regulators, Governments and Concerned Parties:

On May 25, 2018, the General Data Protection Regulation (GDPR) will come into effect. In advance of that date, the domain name community has been working together to ensure systems are prepared and policies are in place.

As that deadline looms, access to the WHOIS system remains unaddressed. ICANN, the multistakeholder organization charged worldwide with the safe, stable and secure operability of the domain name system (DNS), has proposed a model that minimizes its own costs and liability, but does not address the public interest -- omitting a mechanism for access to WHOIS data for law enforcement, cybersecurity and consumer protection needs. This oversight leaves Internet users unprotected and the Internet less stable or secure.

Governments, law enforcement, businesses, intellectual property owners and Internet users worldwide are extremely concerned. ICANN's Governmental Advisory Committee[1] has given consensus advice to the ICANN Board in its ICANN 61 communique to maintain WHOIS to the fullest extent possible and mandate an access mechanism. This view is also held by the ICANN Intellectual Property and the Business Constituencies[2] and the At-Large Advisory Committee[3] within ICANN, and many entities from numerous countries and sectors outside of ICANN.

Accordingly, during the ICANN 61 meeting in San Juan, Puerto Rico, the Business and Intellectual Property Constituencies proposed, and the community discussed, a credible model to ensure continued WHOIS availability for eligible entities seeking data access. Based on feedback from many, including contracted parties (registrars and registries), the model was further refined and is found herein.

Time is of the essence. Should an accreditation and access model not be agreed upon in the next few weeks, the danger is that WHOIS effectively will "go dark" on May 25. Such a development would disable a critical tool employed for the safe and stable operation of the DNS, the prevention of crime, the conduct of vital cybersecurity operations, the protection of consumers, and the enforcement if intellectual property rights. By ICANN's own estimation, a model would not be implemented until at least December 2018 -- causing a prolonged WHOIS access outage.[4]

---

[1] https://gac.icann.org/
[2] http://www.ipconstituency.org/ http://www.bizconst.org/
[3] https://atlarge.icann.org/
[4] See ICANN Global Domains Division presentation at 4:
https://static.ptbl.co/static/attachments/169807/1521130237.pdf?1521130237

To prevent such an outage and its consequences, below is a proposal to provide access for cybersecurity interests and intellectual property owners as well as others charged with protecting Internet users (and can be used by law enforcement, if desired).

We now seek further collaboration from other stakeholders, including contracted parties and ICANN Org, in order to swiftly move this model toward a workable implementation. While this model is proposed for generic top-level domains (gTLDs), we encourage consideration by country code top-level-domains (ccTLDs) as well. We thank you in advance for your help and ask that you please submit your input via email at 3amcomments@gmail.com by 4 April 2018.

Lastly, this work is the result of an iterative process, we continue to evolve the model to accommodate the comments of community members. As such, this descriptive document is intended as the basis for creation of a functional specification for implementation. (For a similar approach, see the TMCH Functional Spec Example[5])

Preface & Overview

This document provides a framework for the rapid implementation of a certification and access model for non-public WHOIS data for legitimate and lawful purposes much like the "tiered access" model proposed in the Expert Working Group's Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS).[6]

Under ICANN's current proposed model,[7] that over-complies with the EU's General Data Protection Regulation (GDPR), public access to WHOIS data elements critical to multiple functions within the DNS will be severely restricted. If adopted, such a restriction will impact the ability of law enforcement, and those involved with consumer protection, to prevent and investigate wrongdoings. This is a significant development, considering:

- Bad actors operate at a global scale, across multiple registrars and top-level domains, sometimes using thousands of names in coordinated and automated attacks.
- Harms range from consumer fraud, disinformation, spam, phishing, botnet attacks, and distributed denial of service (DDOS) attacks to the more grim, including human trafficking and child abuse.
- The harm inflicted is dangerous, painful, irreversible and swift (often measured in minutes and hours), and carries consequences that are problematic for Internet users and others.

---

[5] https://tools.ietf.org/html/draft-lozano-tmch-func-spec-10

[6] Much like the "tiered access" model proposed in the Expert Working Group's *Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS)*, p. 86

[7] https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf

WHOIS data elements are extraordinarily useful in preventing or in investigating and prosecuting against these harms. For example:

- Within WHOIS, a point-of-contact data element, or elements in combination, are often used to expand an investigation beyond a single abused domain to a larger set of jointly controlled and/or connected domains that are used to scale harms exponentially.
- Attribution is critical to minimizing false positives when attempting to discriminate between maliciously and legitimately registered domain names and host names.
- Automated access for a specific legitimate purpose enables surgical, proactive security blocking to prevent spam, phishing attacks, and other abuse from reaching consumers in the first instance.

This model, accordingly, presents an available solution to the problem of access to non-public data elements. Documented here are:

- The types of eligible entities that may seek access to data;
- Legitimate and lawful purposes for accessing data;
- How eligible entities may be accredited to access data;
- A proposed operating model; and
- Terms of accreditation.

Note that this model contains a placeholder for specific provisions for law enforcement agencies (LEAs) and other governmental access. A more detailed outline for such access could be similar to the methods proposed for the other cases, and will be addressed by appropriate government representatives.

Under this model, defined groups of organisations or categories of organisations can gain access to gated data if they (1) require access to data for specific, legitimate and lawful purposes, and (2) are properly validated by a third-party accreditor.

Eligible Entities & Eligibility Requirements

The entities highlighted here are derived from the list of entities and use cases documented in the Expert Working Group's final report on gTLD Directory Services (EWG Report).[8] The three types of Eligible Entities are not an exhaustive list. However, they include those having legitimate and lawful purposes to access data, as well as agents that facilitate protection of public interests, security and lawful behavior.

[8] *Id.* at 21, table of use cases in EWG report

1. Cybersecurity & OpSec Investigators[9]

Eligible Entities include companies, or individuals at companies, who provide cybersecurity or operational security for their company or another corporation, or provide it as a solution and/or service to other individuals, entities or end-users. This category is designed for security companies, organizations that need to protect their own interests and agents/companies that act on their behalf. Agents may include cybersecurity concerns, academic institutions and researchers, OpSec investigators, and cybersecurity data aggregators and others.

Examples of services covered include:

- Identity and access management;
- Application security;
- Fraud protection;
- Digital forensics and incident response;
- Email and data security;
- Protection from spear-phishing and malware, botnets, DDOS attacks;
- Protection for end-users by online platforms, such as browsers, search engines, and social media companies;
- Security intelligence and analytics
- Validation of site ownership to ensure transparency and accountability for commercial activity; and
- Ensuring continuity, integrity and availability of Internet infrastructure.

The application template for applicants in this category includes:

- Identity of the applicant
- Contact information
- Standing for application (organizational mission)
- Evidence of organizational formation or incorporation
- Statement regarding intended use of data

This category of user must also:

- Agree to use the data for legitimate and lawful purposes
- Further agree to:
    - comply with the GDPR and terms of service to prevent abuse of data accessed;
    - be subject to de-accreditation if they are found to abuse use of data; and
    - be subject to penalties under the GDPR.

[9] SSAC members are working to create a proposal for appropriate credentialization of cyber security interests, They are considering models like those used for the Anti-Phishing Working Group (APWG) their APWG Malicious Domain Suspension (AMDoS) model and other relevant security vetting protocols. Other models that could be used include the Trusted Community Representative (TCR) used for DNSSEC.

- Provide:
    - verifiable credentials; and
    - letters of authority/endorsement from governments, companies, and/or individuals on whose behalf they are authorized to act (e.g., hired to protect from security threats including but not limited to spam, malware, malicious apps, denial of service, ex-filtration of content, persistent threats, fraud and other harms).

Examples of entities in this category include: Akamai, BAE Systems, Cloudflare, IBM Security, Sophos, Symantec and security organizations within companies like Salesforce, Facebook, Microsoft.

2. Intellectual Property[10]

This category is designed for intellectual property rights holders, including trademark, patent or copyright owners or their attorneys or agents (agents may include legal representatives, trade associations, data aggregators and brand protection companies) who need to investigate and enforce their intellectual property rights. Applicants in this category may also include members in good standing of a national or state/provincial licensing organization (such as a bar association, or a patent and trademark office), or of a related trade association.

Examples of investigation and enforcement activity include but are not limited to:

- Prevention of consumer confusion through infringement of trademarks
- Abating consumer fraud
- Combating counterfeits
- Preventing the unauthorized distribution of copyrighted material

The application template for applicants in this category includes:

- Identity of the applicant
- Contact information
- Standing for application (organizational mission)
- Evidence of organizational formation or incorporation
- Statement regarding intended use of data

This category of user must also:

- Agree to use the data for legitimate and lawful purposes
- Further agree to:
    - comply with the GDPR and terms of service to prevent abuse of data accessed;
    - be subject to de-accreditation if they are found to abuse use of data; and

[10] The ICANN IPC has been asked to help create a proposal for criteria and credentials that would discriminate against illegitimate use by IP concerns.

- be subject to penalties under the GDPR.

- Applicants must provide:
  - evidence of ownership of intellectual property rights (e.g., a trademark registration);
  - letters of authorization from the rights holders to act on their behalf; or
  - proof of membership in good standing of institutions noted above.

3. [Placeholder for Law Enforcement Agencies & Other Government Agencies]

This is a placeholder for a category that is expected to be addressed by appropriate government representatives on behalf of global, national, regional and local law enforcement agencies and other government agencies charged with protecting public safety and health.

Examples of categories that need investigation and enforcement of applicable law include but are not limited to:

- Fraud
- Theft
- Child abuse
- Human trafficking
- Sale of dangerous and illegal goods and substances
- Hate, racism and discrimination
- Terrorism and threats to national security

Validation and Review of Access Purposes

Accreditations for Eligible Entities will be subject to periodic review by the accrediting authority to ensure they meet the access purpose criteria set forth by that authority. As discussed further below (see Logging), logging should allow analysis of access to non-public Whois data to enable detection and mitigation of abuses and imposition of penalties and other remedies for inappropriate use.[11] Appeal mechanisms will apply in the instance that a review results in de-accreditation.

Legitimate and Lawful Purposes

This section provides a high-level overview of legitimate and lawful purposes for the above accredited Eligible Entities (mapping purposes to entity type). A more fulsome purpose statement, and chart of public interests and legitimate interests pursued by a third party, can be found in ANNEX A.

[11] Much like the "Purpose-Driven Access" model proposed in the Expert Working Group's *Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS)*, p. 10

Legal Actions

- Investigate fraudulent use of registrant's name in any other domain names
- Contact a registrant's legal representative
- Take legal action (e.g., court, administrative or arbitration proceedings)

Intellectual Property Enforcement

- Investigate possible intellectual property infringement
- Contact infringing parties
- Research a domain name's historical record to support IP enforcement
- Identify other domains registered with a given name or address to support IP enforcement
- Initiate or facilitate administrative proceedings

Security / DNS Abuse Mitigation

- Investigate, track and prevent malicious behavior
- Research and investigate security and abuse trends
- Contact victims with compromised domain names
- Enable domain name white/black list analysis by relevant service providers
- Maintain integrity, availability and continuity of online platforms

Contractual Enforcement

- Carry-out contractual compliance investigations
- Conduct registration data escrow audits, and other regulatory and contractual audits
- Validate site ownership and eligibility to conduct commercial activity
- Proof of ownership in domain name purchase/sales transactions

Domain Name Administration

- Transfers of a domain between registrars or registrants
- Confirmation of domain name ownership

Public Health and Safety

- Gather evidence of activity dangerous to public health or safety
- Identify other domains registered with a given name or address that may be involved in activity that threatens public health or safety
- Provide reports related to public health and safety to government agency or law enforcement

<u>All Users</u>

- Must have a specific purpose for their use of non-public data
- Must certify that use of non-public data is legitimate and lawful purposes

- Swear under penalty of perjury that they will not intentionally misuse the non-public data entrusted to them

Purpose and Entity Mapping[12]

Purpose	Entity - Reason
Legal Actions	● Security - To investigate, prevent, remediate fraud, cybercrime ● IP - To investigate, prevent, remediate infringement
Intellectual Property Enforcement	● IP - To investigate, prevent, remediate infringement, fraud
Security / DNS Abuse Mitigation	● Security/IP - To investigate, prevent, remediate criminal activity, fraud, technical exploits
Applicable Law, Regulatory and Contractual Enforcement	● Private Sector IP and Security - for investigation of crimes and DNS abuse for the purpose of protecting users from fraud and assembling data for Law Enforcement Agency response or validating information
Domain Name Administration	● IP - To administer domains ensuring that the domain registration records are under the control of the authorized party and that no unauthorized changes/ transfers are made in the record ● Others - Contracted party usage not in scope, but they and others may need access to ensure chain of custody/ownership of domains for transfers and transactions

Process for Vetting and Accreditation[13]

Users are to be vetted by accreditation authority, based on credentials presented. Contracted parties are not expected to perform vetting.

[12] *Id.* at 21
[13] Note additional scenarios for accreditation - *Id.* at 63

All Eligible Entities must:

- Submit an application with verifiable
    - Contact details
    - Name
    - If Applicant is an agent, the name of individual or entity for whom agency exists
    - Physical Address
    - E-mail Address
    - Telephone number
- Submit required documentation
    - Cybersecurity & OpSec Investigators: Verifiable credentials and letters of authority
    - Intellectual Property: Evidence of IP ownership or a letter of authorization from the rights holder to act on its behalf
- Undergo validation by an ICANN-approved agent (similar to the services offered by certificate authorities or those offered by Deloitte for the trademark clearinghouse)

Once the Eligible Entity successfully completes steps 1 and 2 above, the ICANN-approved agent issues one of two decisions:

- The applicant is issued user credentials or a certificate*
    - Or -
- Rejection of the application

Eligible Entities will be presumed to be qualified for accreditation. However, accreditation can be denied for various reasons, including documentation that is out of order, previous violations of terms of use, or other reasons.

*Any Eligible Entity that receives login credentials must go through annual re-accreditation.

Proposed Operating Model

After over a decade of community work proposing updates to the the existing patchwork Whois system, a modern centralized database solution has not yet been implemented to solve the now immediate problem of access to non-public data in compliance with the GDPR. The operating model proposed here seeks to provide access while making only modest demands on the existing whois systems - meaning that the proposed model can be implemented with existing technologies and with few changes. Later, as efforts to implement RDAP or the new RDS (as envisioned by the EWG) emerge, the methods for access to non-public Whois data for lawful and legitimate purposes may also evolve. However, in the interest of providing pragmatic solutions for interim compliance with GDPR, this proposed operating model follows:

In this proposed model, which is a federated model for access to Whois, eligible accredited entities can present their credentials to any Whois system. Contracted parties collect credentials, which are validated by a central authority, and the requesting entity is either granted

or denied access to data. For example if a credential is expired and not renewed, or has been revoked, access would be denied.

One simple, centralized, expedient and low-touch implementation tactic could be to leverage and extend the existing ICANN centralized Whois system as hosted on the ICANN website found here. Minor modifications could allow gated access to non-public Whois data. This option would achieve the goals of:

1) Uninterrupted service
2) Maintaining the existing Whois system to the greatest extent possible
3) Simplified and consistent implementation
4) Centralized logging

Accredited Users
Upon accreditation, users are given credentials to access Whois data. Users are able to present their credentials to a Whois database operator who validates credentials with a federated, centralized access authority and then provides access to Whois data. Responses to single record queries should be delivered via browsers and automated access should be delivered via port 43 .

Contracted Parties and Agents
Contracted Parties (registries and registrars) will accept credentials and provide access to non-public data for accredited users. They will rely on a centralized access authority to validate user credentials and then provide or deny access. Users will then be able to issue single-record or automated queries against the Whois databases. Once presented with credentials from the accreditation authority, contracted parties cannot unreasonably withhold access to non-public data.

Logging
The query activity of all accredited entities will be logged by the entity that has access to the Whois queries (**logging responsibility decision must be deferred until the technical implementation of the Whois query mechanism is decided -- if contracted parties receive queries, they will have responsibility, if using the ICANN centralized Whois -- they would be responsible for logging**). Logs will include accredited entity, purpose, query, and date. Logs must be retained for a two-year period in a machine readable format and be kept up-to-date with each new query. In the event of an audit or claim of misuse, logs may be requested for examination by an accreditation service or dispute resolution provider. Each query must be mapped to a purpose that is applicable. These steps will allow for auditing of gated data access to minimize abuse and impose penalties and other remedies for inappropriate use, in accordance with terms and conditions explicitly agreed upon by each requestor. Much like proposed in the EWG Report, auditing will drive accountability around things like accuracy and

reliability of registration information and use of gated data for designated purposes only.[14] Note that appropriate restrictions to logs should exist, particularly as applied to accredited LEAs -- "Access to ... logs must be restricted to those trusted, authenticated, authorized individuals and entities with a specific purpose and 'need to know.' … [including] (to monitor RDS compliance with data protection legislation.)."[15]

Abuse Reporting

The system will be suitably transparent to allow appropriate access to third party examination of query rate and volume. A mechanism will be provided for reporting over-extensive use, mirroring or other abuses to the accreditation authority, who will retain the right to investigate and, if necessary, revoke accreditation. The accreditation authority also may refer the offending party to Data Protection Authorities.

Audit

A third-party firm should randomly audit a small sample of query logs for compliance with terms and conditions funded by accreditation and renewal fees. Additionally, Whois database operators may, once annually and at their expense, demand an audit of any accredited entity. A Whois database operator's logs for access may be matched to an accredited entity's logs by a third-party to discern misuse/abuse. (see EWG Report Accountability and Audit Principles[16]) Also, query logs should cite purposes of access, which must be tied to a legitimate and legal use case for each accredited user's use case. Audits will be conducted by a third-party bonded company, and logs are to be delivered with identity of the log origin tokenized or anonymized so that the auditing organization cannot see and thus risk identifying methods of an accredited party. Audit scope may include a request for correspondence sent by accredited entities to registrants as a result of use of non-public Whois data to validate that it was not used for illegitimate purposes including spam.

Accreditation Renewal

Accredited parties must renew their accreditations annually. Renewals will incorporate updated terms of service or other obligations imposed by the accreditation authority. User fees are due and payable upon the date of renewal, with further access conditioned upon successful payment. Accredited parties must provide updated accreditation materials with validity dates covering the period of accreditation. The accreditation authority reserves the right to change the credentials or other material required for accreditation.

Central Access Authority

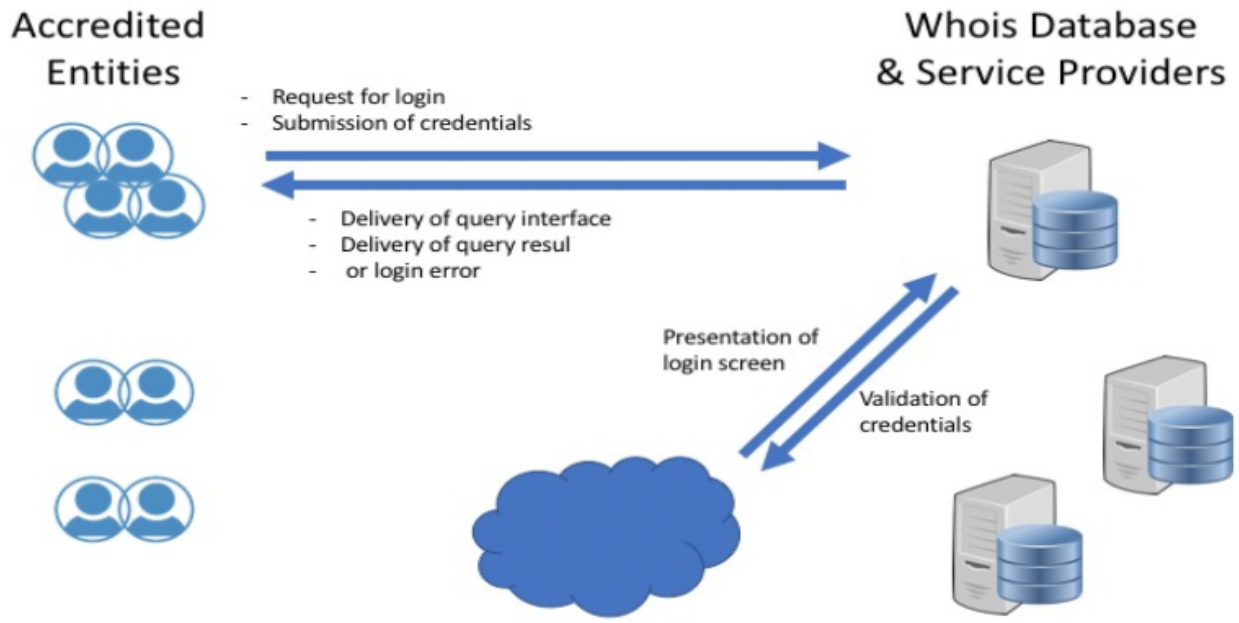
Login and authorization for access by accredited entities to Whois database operators at registries and registrars will be provided by a third-party or parties.

---

[14] *Id.* at 91
[15] *Id.* at 116
[16] *Id.* at 94

Application and renewal fees should be sufficient to cover onboarding and support fees for the authorization and access system. Application and renewal fees should scale with the number of users for each accredited entity. Contracted Parties and Agents should need minimal support to integrate this authorization system into their workflow for gated access.

Federated Access for Whois Diagram



Complaints

- Complaints regarding accuracy of data will be addressed directly to the domain name's sponsoring registrar for resolution.
- Complaints regarding performance of underlying WHOIS providers will be directed to ICANN compliance, who will address the matter with the appropriate registrar, according to the terms of the Registrar Accreditation Agreement.
- All other available remedies (e.g., filing false WHOIS complaints) are available to all appropriate parties.
- Complaints regarding unauthorized access to, or improper use of, data will be addressed to the accrediting agency, who will have the authority to restrict or deny further access to WHOIS data.

Penalties
The accrediting agency will audit non-public data access to minimize abuse and impose penalties and other remedies for inappropriate use, in accordance with terms and conditions explicitly agreed upon by each requestor.

Different terms and conditions could be applied to different purposes. Violation of terms and conditions may result in graduating penalties, including but not limited to:

- Restricted or throttled access
- Denial of further access
- Financial penalties

Terms of Accreditation

Data Protection
Accredited users must protect the personal data in their custody queried from Whois systems and adhere to applicable law for the handling of personal data. At a minimum, individual companies and users have a responsibility to protect data at rest by accessing it on machines that are protected by passwords and have adequate security facility. Similarly, agents acting on the behalf of companies or individuals who have legitimate use of the data have a responsibility to protect the data that they provide to others, and therefore must:

1) Gate access to data via password
2) Secure data at rest through encryption
3) Secure data in transit through encryption
4) Validate with each login that users have up-to-date accreditation for use of the data.

Application Fees
All applicants must pay a non-refundable application fee proportional to the cost of validating an application. Rejected applicants may re-apply up to two times, each time paying the fee. Fees are to be established by validation authority.

Data Access
Accredited data access is to be provided for legitimate uses either for single record queries or automated queries for analysis. Accredited access shall not be rate-limited or otherwise restricted except as needed to ensure operations -- any accredited user may have access to all Whois records from any ICANN contracted party. Data may be stored by accredited users for analysis and collection of case data. Stored data must at a minimum be secured by password and encryption, and use of, and access to, data must conform with terms of service.

Data Misuse
Data is not to be misused in any manner by any party. Categories of misuse could include the following non-exhaustive examples:

- Non-legitimate purposes (e.g., registration data mining for spam/scams)
- Data revealed as a result of a security breach
- Provision or sale of data to non-accredited parties for any reason (unless acting as an accredited agent)
- Use of data for a purpose that is inappropriate for the accredited user type

Data Misuse Penalties

In the event of breach of the terms and conditions, any accredited user's right to access, retain or use data may be suspended. Upon being notified of a breach, a user's access privileges may be revoked, in which case that user must delete any retained data and provide notice to the certifying body that the data has been deleted. Data misuse violations may be appealed to accrediting body (see EWG Report, RDS User Accreditation Principles[17]) and access may be reinstated at the discretion of that body.

Agents (see above) that provide data to other accredited users are responsible for denying access to formerly accredited users whose privileges have been revoked for misuse. Agents are also responsible for validating that users are accredited and maintain accreditation; they must provide access only to currently accredited users or they are subject to misuse penalties.

[17] *Id.* at 62

ANNEX A
PURPOSE STATEMENT FOR THE COLLECTION AND PROCESSING OF WHOIS DATA

The GDPR requires that the collection and processing of personal data be for "specified, explicit and legitimate purposes." (Article 5(1)(b). In addition to processing that is necessary for the performance of a contract to which the data subject—in this case a registrant—is party, the GDPR permits processing that is necessary for the public interest or the legitimate interests pursued by a third party. (Article 6)

The following purpose statement meets the requirements of the GDPR, keeps in line with the proposals of the EWG's final report[18] and ICANN's Cookbook,[19] and supports the public interest and expectation by individual users that the Internet be a safe and secure place by ensuring safety and security through accountability.

The Internet is a public resource governed by a set of private arrangements that replace a system that otherwise would be created by national and international laws. These private contracts, executed under the oversight of ICANN, come with responsibilities, to serve many public policy interests -- especially because (as seen in ICANN bylaws) ICANN's mandates go beyond the mere technical function of mapping names to numbers.

One of these contractual obligations is WHOIS. The WHOIS system plays a key role in accountability online and ICANN needs to adapt the current WHOIS system to comply with the GDPR in line with its new Bylaw commitments requiring that ICANN "use commercially reasonable efforts to enforce its policies relating to registration directory services and work with Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to generic top-level domain registration data, as well as consider safeguards for protecting such data."

As such, in support of ICANN's mission to coordinate and ensure the stable and secure operation of the Internet's unique identifiers, personal data included in domain name registration data may be collected and processed for the following purposes:

[18] *Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS)*, p. 16
[19] The Cookbook, Section 7.2.1, at 34.
https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf

1. Providing access to accurate, reliable, and uniform registration data in connection with the legitimate interests of the registrar and WHOIS system stakeholders;[20]
2. Enabling a dependable mechanism for identifying and contacting the registrant;
3. Enabling the publication of points of contact administering a domain name;
4. Providing reasonably accurate and up-to-date information about the points of contact administering a domain name;
5. Providing access to registrant, administrative, or technical contacts for a domain name to address issues involving domain name registrations, including but not limited to: consumer protection, investigation of cybercrime, DNS abuse, and intellectual property protection;
6. Providing registrant, administrative, or technical contacts for a domain name to address appropriate law enforcement needs;
7. Facilitating the provision of zone files of gTLDs to Internet users;
8. Providing mechanisms for safeguarding registrants' registration data in the event of a business or technical failure, or other unavailability of a registrar or registry;
9. Coordinating dispute resolution services for certain disputes concerning domain names; and
10. Ensuring that ICANN fulfills its oversight responsibilities and preserves the stable and secure operation of the Internet's unique identifier systems through at a minimum, addressing contractual compliance functions (including complaints submitted by registries, registrars, registrants, and other Internet users) as well as other necessary oversight functions, such as reporting, policy development, and implementation.

The following chart ties this purpose statement to the performance of the domain name registration contract between the registrar and the registrant, public interests and legitimate interests pursued by a third party:

[20] GDPR Art. 6(1)(f)

Purpose	Objective	Basis/Interest	Processing	Indicative Users
Domain Name Initial Purchase/ Registration, Management and Control	Tasks within this purpose include creating, managing and monitoring a Registrant's domain name (DN), including creating the DN, updating information about the DN, renewing the DN, deleting the DN, maintaining a DN portfolio, and validating the Registrant's contact information (pursuant to RAA requirements).	Performing and satisfying contractual obligations	-Collection of the data; transfer of data to registry and escrow providers to ensure preservation of data -Inter registrar transfers -Validation of Registrant data for accuracy. - Validation for any restricted TLDs -Zone file provisioning -Storage for retention at least during registration term	Registrants, Registrars, Registry Operators, Escrow Providers, privacy proxy providers, ICANN

Business/Personal Domain Name Purchase or Sale	Tasks within this purpose include making purchase queries about a DN, transferring a DN to another Registrant, acquiring a DN from another Registrant, and enabling due diligence research by the purchaser to ensure that the DN is suitable for purchase and that the seller is bona fide. To accomplish these tasks, the user needs access to the Registrant's Organization and email address, and in some cases additional data – for example, to perform a Reverse Query on the name of a Registrant or contact to determine other domain names with which they are associated.	Prerequisite for functioning marketplace for DNs	-Validating Registrant email contacts for transfers -Contacting Registrant for potential sale - Performing reverse query on registrant information to ensure the sale will meet specific business criteria. -Foregoing requires storage, publication and access of WHOIS data	Registrants, potential DN buyers, resale agents, Registrars

Technical Issue Resolution	Tasks within this purpose include working to resolve technical issues associated with DN use, including email delivery issues, DNS resolution failures, and website functional issues. To accomplish these tasks, the user needs the ability to contact technical staff responsible for handling these issues. (Note: It might be useful to designate multiple points of contact to address various kinds of issues – for example, postmaster for email issues.)	Providing security and stability of the DNS, consumer protection, and protection of Registrants expectation of service Providing a pathway for resolving technical problems/ issues	- Validation of Registrant information -Provision of access to technical users. -Foregoing requires storage of access to technical contact information	Registries, Registrars (Network Operations); DNS service providers; cybersecurity experts
Domain Name Certification	Tasks within this purpose include a Certification Authority (CA) issuing an X.509 certificate to a subject identified by a domain name. Registrants seek certification to increase consumer trust and confidence in their website associated with the DN. To accomplish this task, the user needs to confirm that the DN is registered to the certificate subject; doing so requires access to full WHOIS data	Protecting registrant's interest in maintaining secure DN Providing consumer protection and security	-Validation of registrant contact info for EV, DV, OV SSL certifications -Foregoing requires storage of and access to full WHOIS data	Certificate Authorities, SSL Certification providers, Registrants, Registrars

	about the Registrant.			

Individual Internet User Protection Security and Trust	Tasks within this purpose include identifying the organization/service provider using a DN to instill consumer trust, or contacting that organization to raise a customer complaint to them or file a complaint about them. To accomplish these tasks, the user needs the name of the organization/ service provider (preferably identity-validated) and its email address, and may benefit from following a contact URL to a page that describes the organization/ service provider and its customer service contacts or allows the user to submit a customer service inquiry.	Safety, consumer trust and protection, validation of trustworthiness of the information provider.	-Validation of organization/service provider contact information -Provision of access to consumers and other third parties relying on services/information being provided by the organization/service provider - Foregoing requires storage and publication of and easy access to WHOIS data - Ensuring identity and organizational affiliation of websites conducting commercial activity like accepting credit card or other electronic payments or placing advertisements & promotions	Consumers , online platforms, and the general public

Academic/ Public Interest DNS Research	Tasks within this purpose include academic public interest research studies about DN including public information about the Registrant, the domain name's history and status, and DNs registered by a given Registrant (Reverse Query). To accomplish these tasks, the user needs the ability to access all public data in the WHOIS directory and in some cases may need access to data for use in anonymized, aggregated form.	Promotes broad range of research purposes to improve function, use security, and stability of the DNS; Supports freedom of expression and academic research	- Access to public data and certain non-public data in anonymized form. - Foregoing requires the storage, publication and access to WHOIS data	Students, research orgs, journalists, and academics

Legal Actions	Tasks within this purpose include investigating possible fraudulent use of a Registrant's name or address by other registrants, investigating possible trademark infringement, fraud, copyright infringement, or other civil law violations, contacting Registrant or Registrant's legal representative prior to taking legal action and then taking a legal action if the concern is not satisfactorily addressed. To accomplish these tasks, the user needs the ability to contact the Registrant or its legal representative, without relay through an accredited Privacy/Proxy provider.	Investigating and remediating possible IP infringement or other civil law violations -Preventing fraud and other forms of abuse -Facilitating the establishment, exercise, or defense of legal claims	-Disclose to third party IP rights owners; potential legal complainants - Facilitate identification of and response to fraudulent use of legitimate data (e.g., address) for domain names belonging to the same or other Registrant by using Reverse Query on identity-validated data. -Foregoing requires the storage, retention, publication and access to the full WHOIS data; enabling reverse WHOIS lookup	IP lawyers; intellectual property owners, brand protection and enforcement services companies and associations; cybersecurity experts; Registrars; Registry Operators
Regulatory and Contractual Enforcement	Tasks within this purpose include tax authority investigation of businesses with online presence, UDRP or URS investigation, contractual compliance investigation, and registration data escrow audits. To accomplish this, user needs access to Registrant contact and DN data	-Supports audit and enforcement of private and public legal obligations -Supports security, stability and trustworthiness of DNS	-Storing and disclosing data to regulators, ICANN and authorities entrusted with UDRP, URS adjudication. -Foregoing requires storage, retention and access	Regulators, ICANN Compliance, Parties to contracts, Administrative and enforcement entities such as WIPO

	elements, such as email address and telephone number, as appropriate for the stated purpose. For example, WIPO may need access for UDRP resolution.		to WHOIS data.	

Public Health and Safety Protection and Criminal Investigation	Tasks within this purpose include investigating and reporting threats to public health and safety, including reporting such threats to third party that can investigate and address that threat/abuse, derive investigative leads, serve legal process and/or contact entities associated with a domain name during a criminal investigation. To accomplish these tasks, the law enforcement agent, first responder, public health and safety organizations (e.g. Internet Watch Foundation) needs to quickly and reliably identify the Registrant and all other entities involved with this service provision / maintenance	Public health, safety and security Investigating cyber- crimes and cyber-enabled crimes;	-Detecting abuse by providing access to Registrant data for protecting public health and safety, including by accessing historic full WHOIS data for some period of time -Providing access to Registrant data for the purposes of detecting and mitigating criminal activity, including by accessing historic full WHOIS data for some period of time -Reporting abuse and potential criminal activity, including sharing WHOIS data among multiple public health and safety organizations, organizational and corporate digital crimes teams, law enforcement agencies in multiple jurisdictions to address cross-border nature of abuse/criminal activity	Law enforcement and government or private entities entrusted with enforcement responsibilities; public health and safety organizations, including victim advocacy organizations; digital crime/abuse teams.

			-Foregoing requires storage, retention and access to full WHOIS data; enabling reverse WHOIS lookup to determine breadth and scope of abuse and properly identify person/entity responsible for abuse and/or criminal activity.	

DNS Abuse Study, Investigation and Mitigation	Tasks within this purpose involve identifying the proliferation of malware, botnets, spam, phishing, identity theft, DN hijacking, data hacking, distributed denial of service attacks (DDOS), etc, and deploying mitigation measures to combat such abuses. Tasks in this purpose also include processes that security professionals use to defend their organizations' networks including risk assessing domains that trip alerts on their network (domains attempting to communicate with the network, or for example employees attempting to navigate to websites), as well as correlating WHOIS data with other network telemetry and contextual data they may have on these domains, pivoting from one domain to map resources controlled by active attackers, and if necessary driving to attribution of these attacks to the individuals and organizations behind them.	Protecting Registrant from abuse and hijacking of Registrant's DN Consumer trust in the Internet Ensuring network and information security and stability of the DNS Combating unlawful or malicious/abusive actions negatively affecting secure and stable functioning of the DNS	-Providing access to Registrant data for the purposes of detecting and mitigating DNS abuse -Foregoing requires storage, retention, publication and access to WHOIS data; enabling reverse WHOIS lookup	Law enforcement and public safety agencies; Cybersecurity firms and individual cybersecurity analysts and experts; Online platforms Registry Operators, Registrars ICANN Compliance

ICANN DNS Oversight	Tasks within this purpose involve ensuring that ICANN fulfills its oversight responsibilities and preserves the stable and secure operation of the Internet's unique identifier systems, through at a minimum, addressing contractual compliance functions (including complaints submitted by registries, registrars, registrants, and other Internet users) as well as other necessary oversight functions, such as reporting, policy development, and implementation.	-Promoting choice and competition and ensuring the stability, security, and resiliency of the DNS -Addressing contractual compliance obligations -Supporting audit and oversight functions	Storing and disclosing data to ICANN -Foregoing requires storage, retention, publication and access to WHOIS data	ICANN organization