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 [1]and ICANN's Cookbook,[2] 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:

---

[1] Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS), p. 16, https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf

[2] 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;[3]
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:

[3] 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 about the Registrant.	Protecting Registrant's interest in maintaining secure DN Providing consumer protection and security	-Validation of registrant contact information for EV, DV, OV SSL certifications -Foregoing requires storage of and access to full WHOIS data	Certificate Authorities, SSL Certification providers, Registrants, Registrars

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	Consumers 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 organizations, 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 elements, such as email address and telephone number, as appropriate for the stated purpose. For example, WIPO may need access for UDRP resolution.	-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 to WHOIS data.	Regulators, ICANN Compliance, Parties to contracts, Administrative and enforcement entities such as WIPO

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 -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.	Law enforcement and government or private entities entrusted with enforcement responsibilities; public health and safety organizations, including victim advocacy organizations; digital crime/abuse teams.

DNS Abuse Study, Investigation and Mitigation	Tasks within this purpose involve identifying the proliferation of malware, botnets, spam, phishing, identify 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; 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