Exploring a Unified Access Model for gTLD Registration Data

25 October 2019

TABLE OF CONTENTS

Executive Summary

Following the adoption of the European Union's General Data Protection Regulation (GDPR), the ICANN community and the ICANN organization (org) have worked to balance the law's data protection requirements with the legitimate interests of third parties seeking access to non-public gTLD registration data.

The Temporary Specification for gTLD Registration Data (Temporary Specification) that was adopted by the ICANN Board of Directors and took effect on 25 May 2018 for approximately one year established temporary requirements to allow ICANN and gTLD registry operators and registrars to continue to comply with existing ICANN contractual requirements and community-developed policies in light of the GDPR. It maintained robust collection of registration data, but restricted access to registration data that may include personal data. This presented a significant change from the previous environment in which gTLD registrars and registry operators (collectively, ICANN org's contracted parties) were required, pursuant to their agreements with ICANN org, to publish registration data that often included personal data in publicly accessible directories managed by each contracted party (commonly referred to as Registration Data Directory Services or WHOIS). The ICANN Board noted in the Annex to the Temporary Specification that an important issue for further ICANN community action was the development of "an accreditation and access model that complies with GDPR, while recognizing the need to obtain additional guidance from Article 29 Working Party/European Data Protection Board."

In Phase 1 of an expedited consensus policy development process (Expedited Policy Development Process, or EPDP) the ICANN community developed recommendations for a new ICANN Consensus Policy for gTLD Registration Data based on the Temporary Specification, including purposes for processing registration data. Phase Two of this EPDP (EPDP Phase 2) is underway. In EPDP Phase 2, the ICANN community is considering the development of a system for standardized access to/disclosure of non-public registration data as well as a number of items that were deferred during the EPDP Phase 1 deliberations.

The purpose of this document is to describe a possible model for access to non-public domain name registration data in gTLDs, in order to seek guidance from European Data Protection Authorities (DPAs) on the legal impacts of such a model. In this proposed Unified Access Model (UAM), ICANN org would take on the responsibilities associated with the operation of a central gateway through which requests for access to non-public registration data would be accepted and processed.

This request for guidance, drafted by ICANN org, is informed by the EPDP Phase 2 Team's work to date. Guidance that ICANN org receives from the DPAs regarding the GDPR's application to this UAM will be shared as an input for the EPDP Phase 2 team to inform its work on a system for standardized access to/disclosure of non-public registration data.

The model proposed in this paper is not intended to replace the ICANN community's policy development process. Rather, ICANN org seeks to address and help clarify the legal foundation upon which a model could be built, so that this information can be factored into the ICANN community's ongoing policy work. Additionally, ICANN org seeks to respond to a range of communications, including the EDPB's statement on 27 May 2018, which noted it "expects ICANN to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders."

1 Background

Domain Name Registration Data Serves Critical Public Interest Function

In a hierarchical and decentralized system like the Internet, which is a network of networks, it is important for the entities who operate the pieces within it to be able to contact the actors to warn of problems or coordinate responses to operational issues. Domain name registration data is a critical tool for identifying the actors behind domain names. Domain name registration data includes personal directory-type information, such as a registrant's name, postal address, email address, and telephone number, as well as other non-personal data, such as information about the domain name registrar.[1]

Access to registration data, commonly known as WHOIS data, serves the public interest and contributes to the security and stability of the Internet by providing contact information to support efforts related to consumer protection, cybercrime investigation, DNS abuse, and intellectual property, and to address appropriate law enforcement needs. Registration data also enables network administrators and others to identify and correct system problems and to maintain Internet stability. Domain name registration data can be used to determine domain name availability, combat spam and fraud, prosecute trademark infringement, and enhance the accountability of domain name registrants.

The ICANN Bylaws[2] provide that ICANN shall use commercially reasonable efforts to enforce its policies relating to the Registration Directory Services (RDS) and shall work with its Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to gTLD registration data as well as consider safeguards for protecting such data. The Bylaws further recognize the need to ensure that ICANN's implementation of RDS requirements meets the legitimate needs of law enforcement, promoting consumer trust, and safeguarding registrant data.

Approximately 2,500 different legal entities around the world (the contracted parties) have their own subset of the global, decentralized RDS for gTLDs, commonly known as WHOIS. There is no single, centralized database of this data. With the adoption of the Temporary Specification and the subsequent gTLD Registration Data Policy recommended by the ICANN policy development process, WHOIS data will migrate to a new RDS protocol known as Registration Data Access Protocol or RDAP.[3] There are different types of registration data that cover the 354.7 million domain names[4] registered around the world. ICANN policy and contractual requirements, which govern the

[1] See Appendix: Registration Directory Services Record Fields for details of which fields appear in a record, and which data is publicly displayed in the RDS.
[2] See ICANN Bylaws, Section 4.6(e), https://www.icann.org/resources/pages/governance/bylaws-en/#article4.
[3] RDAP enables users to access current registration data and was created as an eventual replacement for the WHOIS protocol. RDAP was developed by the technical community in the Internet Engineering Task Force (IETF). RDAP is a protocol that delivers registration data like WHOIS, but its implementation will change and standardize data access and query response formats. RDAP has several advantages over the WHOIS protocol, including support for internationalization, secure access to data, and the ability to provide differentiated access to registration data.
[4] See https://www.verisign.com/assets/domain-name-report-Q22019.pdf.

practices of gTLD domain name registries and registrars, cover approximately 206 million of those names. The remaining names belong to country code TLD operators, which set their own RDS policies. There are also RDS systems that cover IP addressing and other numbers, which set their own policies.

Temporary Specification Limits Public Availability of gTLD Registration Data

The Temporary Specification[5] significantly changed ICANN's requirements for the contracted parties' public display of registration data, as part of ICANN's efforts to bring the requirements into compliance with the GDPR. Prior to the adoption of the Temporary Specification, the contracted parties were required under their respective agreements with ICANN org to publicly display contact information for domain name registrants (for example, their name, email address, phone number, and postal address) by default, unless the registrant had taken steps to shield that data from public access, for example, by utilizing a privacy or proxy domain name registration service.[6]

The ICANN Board adopted the Temporary Specification to keep ICANN's contracted parties in compliance with the requirements of the GDPR, as well as with ICANN's contractual requirements concerning registration data.

Now, most directory information contained in gTLD domain registration data is no longer publicly available. Parties seeking access to non-public gTLD registration data must request that access from the contracted parties. Contracted parties are required to provide reasonable access to personal data in registration data on the basis of a legitimate interest pursued by the third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the registered name holder or data subject pursuant to GDPR Article 6(1)(f). Each contracted party conducts its own assessment to determine whether a request for access will be granted. This has fragmented a system that many rely upon for reasons as varied as law enforcement investigations, intellectual property, and security incident response, among others.

[5] The Temporary Specification is now an interim ICANN Consensus Policy, pending ICANN org's implementation of the Consensus Policy recommendations of the Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data, https://www.icann.org/resources/pages/interim-registration-data-policy-en.

[6] ICANN org was directed by the ICANN Board to implement a new accreditation program for privacy and proxy service providers, pursuant to policy recommendations developed by a community Policy Development Process (PDP) working group (See https://gnso.icann.org/sites/default/files/filefield_48305/ppsai-final-07dec15-en.pdf). That working group defined a "privacy service" as "a service by which a Registered Name is registered to its beneficial user as the Registered Name Holder, but for which alternative, reliable contact information is provided by the privacy or proxy service provider for display of the Registered Name Holder's contact information in the Registration Data Service (WHOIS) or equivalent services. The working group defined a "proxy service" as "a service through which a Registered Name Holder licenses use of a Registered Name to the privacy or proxy customer in order to provide the privacy or proxy customer use of the domain name, and the Registered Name Holder's contact information is displayed in the Registration Data Service (WHOIS) or equivalent services rather than the customer's contact information." The implementation of this program is currently on hold, pending the completion of EPDP Phase 2. See: https://www.icann.org/en/system/files/correspondence/namazi-to-drazek-et-al-05sep19-en.pdf.

EPDP Phase 1 Recommends New Policy

The EPDP developed a new consensus policy on gTLD registration data, and concluded Phase 1 of its work in March 2019. The ICANN Board adopted 27 of the 29 new policy recommendations in May 2019. Overall in Phase 1, the EPDP took two actions. First, the EPDP Phase 1 team recommended a new policy concerning gTLD registration data. Second, the EPDP Phase 1 team recommended that the ICANN Board adopt the Temporary Specification as an Interim gTLD Registration Data Policy, pending the implementation of the EPDP Phase 1 team's recommended new registration data policy. This Interim Registration Data Policy became effective 20 May 2019.

The new registration data policy recommended by the EPDP Phase 1 team defines specific purposes and legal bases for the processing of gTLD registration data that is required under the policy, including data collection, retention, escrow, and transfer of data to third parties (such as data escrow agents and dispute-resolution service providers) and from registrars to registry operators. Based on those specified purposes, the policy identifies what data must be collected, retained, and displayed in the publicly available RDS, and what non-public registration data may potentially be disclosed to third parties when the requirements for disclosure are met. It is expected that the new registration data policy recommended by the EPDP team in Phase 1 will be implemented in 2020.

EPDP Phase 2, now underway, is focused on developing policy for who can have access to non-public gTLD registration data, under what circumstances, and which data fields may be disclosed, among other variables, in addition to other policy questions that were deferred from Phase 1.

One of the policy questions deferred from the EPDP Phase 1 was the EPDP team's recommendation to include a purpose specifically related to third-party access to registration data, known as "purpose two." The EPDP Phase 1 team recommended the following ICANN purpose for the processing of personal data contained in gTLD registration data: "Contributing to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission through enabling responses to lawful data disclosure requests." The ICANN Board has not adopted this recommended purpose[7] due to the EPDP Phase 1 team's characterization of this as a placeholder. The European Commission in a 17 April 2019 letter and 3 May 2019 letter to ICANN org recommended "*revising the formulation of purpose two by excluding the second part of the purpose 'through enabling responses to lawful data disclosure requests' and maintaining a broader purpose to 'contribute to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission,' which is at the core of the role of ICANN as the 'guardian' of the Domain Name System.*"

Support for Registration Data Access Solution

To address the fragmentation of registration data access that was created upon the adoption of the Temporary Specification, and which has continued with the implementation of the Interim Registration Data Policy, many ICANN stakeholders supported the idea of exploring a unified mechanism for accessing non-public registration data.[8]

[7] See https://www.icann.org/en/system/files/files/epdp-scorecard-15may19-en.pdf.

[8] See, for example: https://www.icann.org/en/system/files/correspondence/bunton-diaz-to-chalaby-marby-22oct18-en.pdf.

The European Commission has called this work "vital and urgent" and urged ICANN org to expeditiously address this issue. The Commission wrote in a 3 May 2019 letter to ICANN org that "the current situation where access to non-public registration data for public policy objectives is left at the discretion of registries and registrars affects the EU Member States authorities' ability to obtain legitimate access to non-public registration data necessary to enforce the law online, including in relation to the fight against cybercrime." The Commission added that, "[t]he need to ensure effective and secure treatment of third party access requests requires therefore ICANN and the community developing a unified method for accessing non-public gTLD registration data." The EU and its Member States have supported "the development of a unified access model that applies to all registries and registrars and provides a stable, predictable, and workable method for accessing non-public WHOIS data for users with a legitimate interest or other legal basis as provided for in the GDPR, including law enforcement authorities and other public enforcement authorities, including for cybersecurity purposes (e.g. consumer protection and public safety agencies)."[9] They have also supported "the on-going dialogue between ICANN and the EU data protection authorities to ensure that data processing activities in the context of WHOIS are in line with the EU data protection rules."[10]

ICANN's Governmental Advisory Committee (GAC), which serves as the voice of governments and international governmental organizations within ICANN, and includes 178 members and 36 observers, has also emphasized the need for a unified access model. In advice[11] to the ICANN Board, the GAC, "urged ICANN to take all steps necessary to ensure the development and implementation of a unified access model that addresses accreditation, authentication, access and accountability, and applies to all contracted parties." In addition, the G7's High Tech Crime Subgroup, in a letter to ICANN, supported the GAC's advice and emphasized the importance of developing a unified access model as "a necessity for public safety."

Post-GDPR Efforts Related to Registration Data Access

In June 2018, ICANN org published a discussion document titled, Framework Elements for a Unified Access Model for Continued Access to Full WHOIS Data. Building on that discussion document as well as various inputs from the community[12] and the European Data Protection Board (EDPB),[13] ICANN org published the Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data – For Discussion in August 2018.

To address governmental and ICANN community support for exploring such a model, ICANN's CEO formed a Technical Study Group (TSG) to explore technical solutions for providing access to non-public registration data. The TSG published "TSG01, Technical Model for Access to Non-Public Registration Data" on 30 April 2019 and submitted this to the ICANN CEO and President for further consideration. The TSG's technical model is based on RDAP, the replacement protocol for WHOIS. In the TSG model, a requestor would authenticate their identity and legitimate purpose for requesting nonpublic data and submit their request for nonpublic data to a central service that would approve or deny the request. If approved, the central service operator would ask the relevant gTLD

[9] See http://data.consilium.europa.eu/doc/document/ST-13443-2018-INIT/en/pdf
[10] *Ibid*
[11] See https://gac.icann.org/contentMigrated/icann63-barcelona-communique
[12] See https://www.icann.org/resources/pages/gdpr-comments-2018-04-04-en.
[13] See https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf.

registry and/or registrar to provide all domain name registration data to the central service. In turn, the central service operator would filter it and return the appropriate data subset to the requestor.

The UAM proposed in this paper is based on the TSG's technical model. Some of the assumptions made in this model, such as a requirement that requests for nonpublic data be routed through a central service, may be implemented as a matter of policy based on the EPDP Phase 2 team's recommendations.

The EPDP Phase 2 team is currently considering whether to recommend specific requirements for access to data based on specific use cases. Use cases under consideration by the EPDP Phase 2 team include multiple scenarios related to criminal law enforcement, non-law-enforcement investigations and civil claims, and consumer protection/abuse prevention/network security.

2 Purpose of Dialogue With European Data Protection Board

In this paper, ICANN org proposes an approach for a Unified Access Model (UAM) based on the technical model proposed by the TSG, for discussion with the DPAs. The proposed UAM would provide a centralized system for access to non-public registration data, creating a transparent and predictable system for data subjects and parties requesting access to non-public registration data. In this UAM, ICANN org would take on the responsibilities associated with the operation of a central gateway through which requests for access to non-public registration data would be accepted and processed. This paper aims to test the theory that such a system would consolidate responsibilities related to the processing activity of disclosure of non-public registration data within the proposed UAM.

A necessary element to ensure that natural persons have control of their own personal data is knowledge of what data is held, by whom, for how long, and when and under what conditions such data may be processed and/or shared with third parties. The ICANN community, through the recommendations of the EPDP Phase 1 Team, has endeavored to ensure that domain name registrants have the requisite control over their personal data in the distributed domain name ecosystem, comprised of nearly 2,500 contracted parties. The implementation of a unified method for disclosure of non-public registration data could take this a step further.

Under the EPDP Phase 1 policy, registrants must be informed about the applicable arrangements concerning the processing of their personal data, including the standards that each individual registrar and registry operator will apply in response to a request for access to a registrant's non-public registration data.[14] However, each contracted party will individually apply the standards for access (for example, in determining whether a specific request is lawful and whether such data should be disclosed). If identical requests for non-public data are sent to a registry operator and a registrar concerning the same domain name and alleging the same legal basis for access, such requests may be answered differently based on the registry operator's and registrar's application of

[14] EPDP Phase 1, Recommendation 18, states that, "Registrars and Registry Operators must publish, in a publicly accessible section of their web-site, the mechanism and process for submitting Reasonable Requests for Lawful Disclosure. The mechanism and process should include information on the required format and content of requests, means of providing a response, and the anticipated timeline for responses." See https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf

the same criteria and balancing of the competing interests at stake, where applicable. This could create uncertainty for data subjects over when their personal data may be disclosed to a third party, and under what conditions.

The individual application of standards for access in response to a disclosure request to a registrar or registry operator could also create misgivings for data subjects whose personal information is published on a website unlawfully. Individuals who want to address a complaint to a website that publishes their personal data directly or supervisory authorities investigating a complaint by a data subject can face challenges in obtaining access to the non-public information for the domain's registrant from the registry or registrar with which the domain of a website is affiliated, so as to seek remedy. This could hinder the data subject's exercise of privacy rights and the supervisory authority's ability to enforce privacy laws.

A UAM could ensure that uniform standards and processes for third-party access to registrants' personal data are developed and consistently applied across the gTLD domain name ecosystem. Under a UAM, a registrant could be clearly informed and understand when the registrant's personal data would, and would not, be disclosed.[15] The registrant would have a single point of contact who would be responsible for disclosing any data and identifying what protections would be applied and where to seek redress if something went wrong. It would be easier to ensure transparency in a single, unified system as compared to the current fragmented situation. Moreover, a system with fewer actors can be more easily secured.

In addition to benefits to data subjects, a centralized system would successfully meet the important public interest goals that legitimate access to non-public registration data serves for all parties involved. Under the current fragmented situation, disclosure of non-public registration data to third parties with legitimate purposes can be significantly delayed, and cases have been reported in which access has been denied to third parties that were able to establish legitimate interest for requesting disclosure of registration data. This can result in law enforcement bodies facing difficulties when investigating a crime; consumers being deceived online by fraudulent websites, while intellectual property rights holders seek ways to find and contact the people behind fraudulent websites; and IP infringements and cyber attacks not being mitigated in a timely manner.

This fragmentation and inconsistency stems from the fact that each of the 2,500 contracted parties must make an individual decision in response to a request for access to registration data and apply their own criteria and balancing of the competing interests at stake.

If ICANN's contracted parties must continue to make individual decisions in response to each request for registration data, the situation would necessarily continue to be unpredictable, inconsistent, and would fail to meet important public interest goals for all parties involved, including data subjects. ICANN's hypothesis is that the only way to create a predictable and consistent practice is to put in place a UAM that removes the responsibility for the acts of (a) making decisions about disclosure of non-public data and (b) disclosure of that data from the contracted parties and

[15] The EPDP Phase 2 team is considering specific use cases for an access model, for which processes and criteria for requests and responses could be standardized and potentially automated to some extent, such as "Investigation of criminal activity against a victim in the jurisdiction of the investigating EU LEA requesting data from a local data controller," "Identify owner of abusive domains and other related domains involved in civil legal claims related to phishing, malware, botnets, and other fraudulent activities," and "Trademark owners requesting data in the establishment, exercise or defense of legal claims for trademark infringement." Full list of use cases currently under consideration is available at https://community.icann.org/display/EOTSFGRD/d.+Use+Cases.

consolidates it within a UAM. This UAM is proposed as a mechanism to centralize responsibilities associated with the disclosure of personal data contained in gTLD registration data and increase consistency of responses. In addition, a UAM in which the responsibility for vetting data requests and disclosing data is centralized may reduce the likelihood of GDPR breaches occurring. A system with fewer actors and thus fewer points of failure may be easier to consistently secure, hold accountable and risk-assess. It could also be easier to ensure the system is transparent to data subjects and data protection authorities, and can efficiently be modified in response to adverse incidents, decisions, or court rulings.

This proposed UAM is not intended to impact the contracted parties' GDPR responsibilities outside of the UAM; for example, responsibility for a data breach unrelated to the UAM. The UAM will not and cannot exclude the possibility that third parties might bring claims for access to non-public registration data directly against registry operators and registrars.

The goal of dialogue on the proposed UAM is to obtain guidance from the DPAs regarding the contracting parties' roles and responsibilities under the GDPR with respect to the processing of registration data in the course of disclosing such data to a third party through this proposed UAM.

Any input provided from the European authorities will be shared with the EPDP Phase 2 team to help guide its work in developing a standardized system for access and disclosure.

3 Key Concepts

The UAM outlined in this paper is based on these key concepts:

a. **Accreditation**: The process or action of recognizing a person as having a particular identity, possibly with an associated affiliation or status. The UAM would require each *Requestor* to verify that it is accredited prior to the system processing a request for non-public data. Once the identity and the role of the *Requestor* have been verified, credentials[16] for the UAM system would be established for the verified *Requestor.* This function would be performed by an actor called the *Identity Provider*.

b. **Authentication**: The process or action of verifying the identity of a *Requestor* when a request for registration data is made. In this UAM, this function is performed by an actor called the *Identity Provider* (See Section 4, UAM Roles). The *Requestor* must be accredited prior to being authenticated.

c. **Authorization**: The process of determining whether queried data may be disclosed to a certain (authenticated and accredited) *Requestor*. In this UAM, this is the process of securely granting access to non-public gTLD registration data to accredited *Requestors* (e.g., John Doe as a law enforcement agent is granted access to data from a given domain name). This function is performed by an actor called the *Authorization Provider*[17] (See Section 4, UAM Roles). Users and their roles must be *Authenticated* before they may be *Authorized*.

[16] Credentials are described in greater detail in TSG01: https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf

[17] The TSG Report called this role "Third Party Authorizer."

Authorization to access non-public registration data could be granted on a per-request basis[18] for *Authenticated Requestors*.[19]

d. **Registration Data**: Registrars are required, pursuant to their agreements with ICANN org, to collect and maintain certain *Registration Data* about each gTLD domain name and to transfer certain registration data to the relevant registry operator and a data escrow agent. The required *Registration Data* (including registrant name, organization, and contact information) may concern legal and/or natural persons, and may be collected by the registrar from the data subject or a third party[20].

e. **Registration Data Access Protocol (RDAP)**: *RDAP* enables users to access current registration data and was created as an eventual replacement for the WHOIS protocol. *RDAP* is a protocol that delivers *Registration Data* like WHOIS, but its implementation will change and standardize data access and query response formats. *RDAP* has several advantages over the WHOIS protocol, including support for internationalization, secure access to data, and the ability to provide differentiated access to *Registration Data*. Registries and registrars have been required to implement an *RDAP* service since 26 August 2019.

4 UAM Roles

The UAM outlined in this paper describes several key actors and the roles they would play:

a. **Authorization Provider*:*** The party evaluating a given query and the identity of the *Requestor* against the policy governing access to non-public registration data. The evaluation yields approval or rejection based on how the policy is applied. The model allows for one or more *Authorization Providers*, either for all *Requestors* or by subsets of requests based on similar characteristics.[21]

[18] The TSG Report also considered the technical feasibility of offering authorization per user, i.e., that a user would be granted access to any domain names once the user is accredited.
[19] This is a policy question that is beyond the scope of this proposal, and will be considered in EPDP Phase 2. The EPDP Phase 2 team is considering specific use cases for an access model, for which processes and criteria for requests and responses could be standardized and potentially automated to some extent, such as "Investigation of criminal activity against a victim in the jurisdiction of the investigating EU LEA requesting data from a local data controller," "Identify owner of abusive domains and other related domains involved in civil legal claims related to phishing, malware, botnets, and other fraudulent activities," and "Trademark owners requesting data in the establishment, exercise or defense of legal claims for trademark infringement." Full list of use cases currently under consideration is available at https://community.icann.org/display/EOTSFGRD/d.+Use+Cases.
[20] Registrars may also collect additional *Registration Data* at their discretion, but this is beyond the scope of this UAM, as it is outside the data ICANN requires gTLD registries and registrars to collect as part of its contracts.
[21] For example, depending on what ICANN's policy development process deems appropriate, different groups of users such as intellectual property rights' holders, cybersecurity researchers, and law enforcement agents

b. **Contracted Parties:** gTLD registries and registrars that have a contract with ICANN org to operate a gTLD registry, and to offer registration services to end users, respectively. Starting on 26 August 2019, *Contracted Parties* were required to offer an RDAP service.[22]

c. **Central Gateway:** Central service to which queries for non-public *Registration Data* in gTLDs are submitted and through which responses are provided. In this model, ICANN org serves as the *Central Gateway* operator. The *Central Gateway* interacts with *Identity Provider(s)* and *Authorization Provider(s)* to *Authenticate* the *Requestor* and confirm they are approved to receive the data they requested, respectively. The service consists of two sub-services: a web portal and an *RDAP* server.

d. **Identity Provider:** The party that accredits *Requestors* to verify their identity and role, then establishes their credentials in the system. Once a user is established in the system, an *Identity Provider* would confirm that a *Requestor* has been *Authenticated* before a given query can be evaluated for approval or denial. The model allows for one or more *Identity Providers*, for either all types of *Requestors* or some subset.[23]

e. **Requestor:** A person in a specific role who submits queries (e.g., John Doe as law enforcement agent), which may gain them access to non-public gTLD *Registration Data*.

f. **Centralized System**: The collective of Central Gateway, Identity Provider(s), and Authorization Provider(s).

5 Proposed UAM

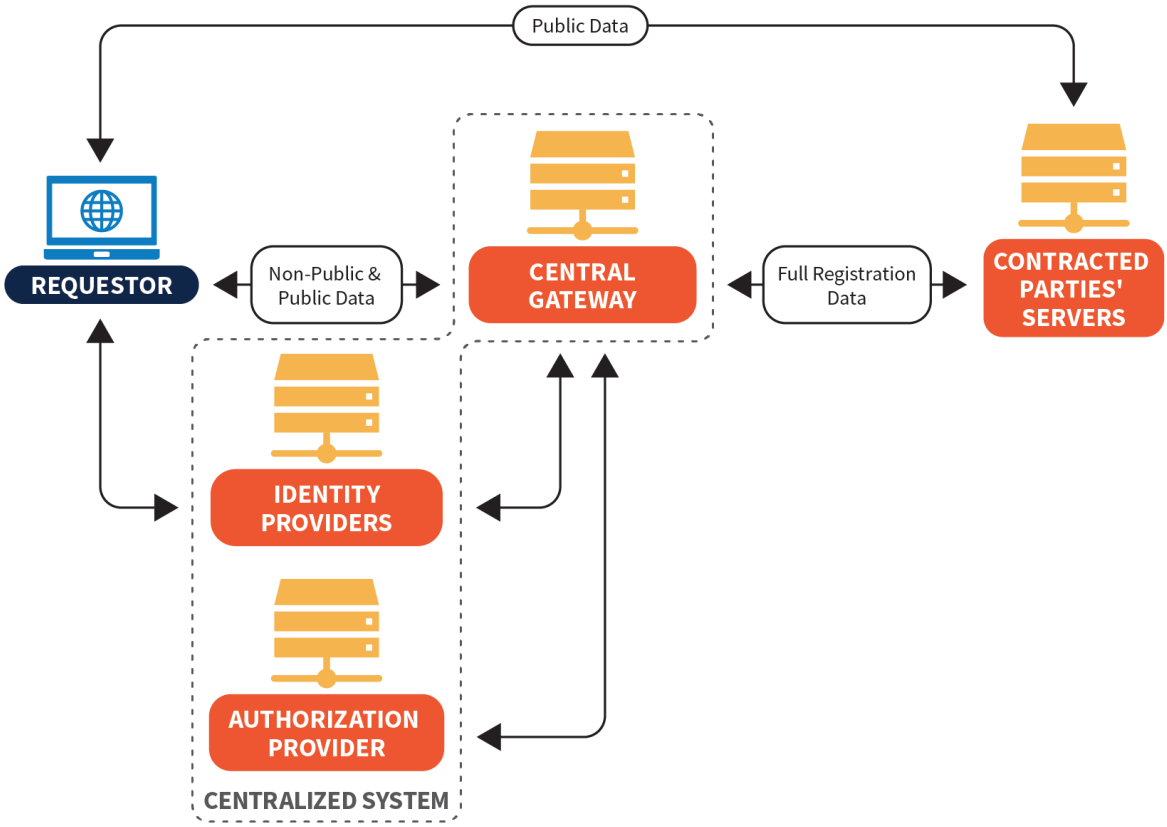
The proposed UAM is described in detail below. To ensure a reliable system, Service Level Agreements (SLAs) will be established for each party that operates the elements of the system. These SLAs would define the service performance levels expected of each party and the penalties for failing to meet them.

could be served by different entities. Alternatively, a single entity may serve all those who seek to use the system.

[22] Per the Interim Registration Data Policy for gTLDs, by default, most Contracted Parties offer redacted Registration Data in WHOIS and RDAP.

[23] For example, different groups of users such as intellectual property rights' holders, cybersecurity researchers, law enforcement agents can be served by different entities. Alternatively, should ICANN's policy development process deem it appropriate, a single entity may serve all those who seek to use the system.

The following graphic provides an overview of the proposed UAM:



Step 1: Accreditation. Before a *Requestor* may submit any request, it must be *Accredited* to comply with relevant policy requirements, e.g., that the *Requestor* may query non-public *Registration Data* and that they must comply with other eligibility criteria in order to set up credentials that will enable them to be securely *Authenticated* when submitting requests.

One or more *Identity Providers* would perform this task.

Step 2: Accredited Requestor Requests Registration Data From Central Gateway. In this proposed UAM, a single entity (ICANN org) would operate a *Central Gateway* offering an *RDAP* service and a human-friendly web service. *Requestors* could use either service. All requests for non-public *Registration Data* (which includes, for example, registrant name, organization, postal address, email address, phone number) processed through this UAM must be submitted through the *Central Gateway*. Each request would be limited to registration data related to a single domain name.

Step 3: Authentication. The *Central Gateway* would redirect the *Requestor* to the corresponding *Identity Provider* for the *Requestor* to be authenticated. If the *Requestor* is successfully authenticated they will be provided with a token and redirected to the *Central Gateway* again. The *Central Gateway* would receive and validate the token, which would allow it to securely confirm the identity of the *Requestor*.

Step 4: Authorization. Once the *Requestor* has been authenticated, the *Central Gateway* would contact the relevant *Authorization Provider*, providing the identity of the *Requestor,* the request, and

any other information deemed necessary by policy to evaluate a request. The *Authorization Provider* would evaluate those parameters against the appropriate policy. If the request meets the requirements of the policy, the *Authorization Provider* would reply to the *Central Gateway* with another token. The *Central Gateway* would validate this token to securely learn the result of the *Authorization Provider's* determination.

Step 5: Gateway Request Sent to Contracted Party. If the request is authorized, the *Central Gateway* would contact the relevant *Contracted Party* servers, *Authenticate* itself to them, and request the *Registration Data* of the relevant domain name.

Step 6: Contracted Party Disclosure to Central Gateway. After authenticating with the *Central Gateway*, *Contracted Party* servers would provide the full *Registration Data* set for the queried domain to the *Central Gateway*. The identity of the *Requestor* would not be shared with the *Contracted Parties*.

Step 7: Central Gateway Parses Relevant Dataset. After obtaining the full *Registration Data* set from the *Contracted Parties*, the *Central Gateway* would parse the data based on the *Requestor's* access criteria, as determined by the relevant policy.

Step 8: Gateway Discloses Data to Requestor. After parsing the data, the *Central Gateway* operator would provide the *Requestor* with the *Registration Data* set that is appropriate according to the relevant policy. For example, if the policy specifies that law enforcement is granted access to all non-public *Registration Data* fields, then the answer from the *Central Gateway* would include all of those fields. If the policy indicated that another category of *Requestor* is only entitled to a subset of non-public *Registration Data*, e.g. registrant email address, then only that data element, plus all other elements that are publicly available, would be disclosed.

Step 9: Gateway Operator Discards Data. All *Registration Data* would then be discarded by the *Central Gateway*.

6 Personal Data Processing Activities During Disclosure Requests

Each data processing activity within the UAM must have adequate legal basis to support it. This will depend on who performs the processing and for what purpose, and will be determined based on the recommendations developed through ICANN's policy development process.

The various processing activities contained in the aforementioned Steps 1-9 are carried out by the relevant parties of the UAM: *Central Gateway*, *Identity Providers*, *Authorization Providers*, *Requestors,* and *Contracted Parties*. Irrespective of whether these parties are acting as joint or independent controllers or as a processor on behalf and at the direction of a controller, they are responsible for ensuring compliance with all applicable legal and policy requirements, including ensuring a legal basis for the relevant processing activity.[24]

[24] Guidelines for applying the "balancing test" for specific use cases are expected to be considered by the EPDP Phase 2 team and would be explored during the implementation of any access model recommended by the EPDP Phase 2 Team. Generally, the role of the Contracted Parties in a UAM will depend on their control over the purposes and means of each act of processing that occurs within the UAM. It is possible that,

For ICANN org, in taking responsibility for operation of the *Central Gateway,* as well as the *Identity Providers* and *Authorization Providers* (if these roles are performed by private organizations), the legal basis for the processing would be legitimate interests (Art. 6 (1) f GDPR). Legitimate interests of the *Central Gateway*, the *Identity Providers* and the *Authorization Providers* would include contributing to a stable and secure domain name system. In instances in which *Identity Provider*s and *Authorization Providers* are EU or EU Member State public authorities, these entities may be able to rely on the legal basis that processing is necessary for the performance of a task carried out in the public interest (Art. 6 (1) e GDPR), assuming EU or Member State law defines their tasks accordingly (Art. 6 (3) GDPR).

The legal basis for each *Requestor* would depend on the nature of a request. EU or EU Member State public authorities might rely on a legal basis provided for in EU or Member State law (Art. 6 (1) e GDPR). Private organizations might rely on legitimate interests of, for example, establishment, exercise, or defense of legal claims or IT security interests.

Contracted Parties, depending on the circumstances, might rely on Article 6(1)f or Article 6(1)c GDPR as the basis for their processing of registration data within a UAM. Contributing to a stable and secure domain name system is a legitimate interest on the part of the *Contracted Parties,* as well.[25]

In particular, for purposes of the GDPR, the following activities within the proposed UAM may involve processing personal data contained in gTLD *Registration Data*, and must have a legal basis.

A. When a *Contracted Party's* server discloses non-public gTLD *Registration Data* to the *Central Gateway.* In this proposed UAM, the *Contracted Party* discloses the full *Registration Data* set[26] for the single requested domain name to the *Central Gateway*, as opposed to a more limited set of the registration data (the specific data-set which the *Requestor* is *Authorized* to receive under the governing policy), because:

i) Release of the full data set minimizes the *Contracted Parties'* visibility into the request. If a more limited data set is released, this may reveal characteristics of the *Requestor* to the *Contracted Party*.
ii) Release of the full data set would preserve operational secrecy in cases requiring it by not revealing to the *Contracted Party* that the *Requestor* is a specific type of *Requestor*, such as a law enforcement authority.
iii) Release of the full data set simplifies the disclosure process.

depending on the policy recommendations, the Contracted Parties might not be considered controllers, but processors when transferring registration data into a UAM.

[25] Please refer to Question 2, in Section 8, below, and the accompanying footnote.

[26] Domain name registration data exists across thousands of registrars and registries. There is no centralized database of records. Requests for data processed through this UAM must be made for each individual domain name. Bulk requests -- or requests for registration data on multiple domain names in a single request -- would not be possible in this system. Non-public data includes, but is not limited to, the registrant's name, organization, street address, city, postal code, phone number, and e-mail address, as well as the technical contact's name, phone number, and email address. The registrant's state/province and country remain publicly available.

iv) Passing data through a central gateway makes the overall system more secure; it is easier to implement appropriate technical measures to ensure the security of the processing in one centralized system, as opposed to a decentralized system.

As discussed earlier, the transfer of non-public *Registration Data* from a *Contracted Party* to the *Central Gateway* can be based upon legitimate interests (Art. 6 (1) f GDPR).[27] It is necessary to disclose the full *Registration Data* set in this context, as otherwise a central feature of the UAM, shifting the decision-making power over an individual access request to the extent possible from a *Contracted Party* to the *Central Gateway* (acting together with the *Identity Providers* and *Authorization Providers* in evaluating the access request), cannot be achieved.

The *Contracted Parties* cannot be informed about the background of an individual access request nor about the *Requestor*, as they could otherwise be expected to raise objections, which bears the risk of fragmentation. In this scenario, the *Contracted Parties* could also potentially be regarded as responsible controllers with respect to the actual disclosure decision made by the *Central Gateway* (together with *Identity Providers* and *Authorization Providers*), a situation of possible joint control with the *Contracted Parties* that would undermine the goal of the UAM. As a consequence the full *Registration Data* set needs to be disclosed to the *Central Gateway.* This will not only technically simplify the disclosure process, but is also necessary to ensure the confidentiality of the access request, as mentioned in the foregoing.

Transferring the full *Registration Data* set does not amount to bulk access to *Registration Data*, as *Registration Data* sets will be transferred on a case-by-case basis upon individual request of the *Central Gateway*. There is no ongoing access of the *Central Gateway* to all *Registration Data* sets of a *Contracted Party*, nor will the *Central Gateway* store all *Registration Data* sets centrally. Rather the *Registration Data* sets will be deleted without undue delay if an access request has been addressed.

B. When the *Central Gateway* parses *Registration Data* based on the *Requestor's Authorization* to access the data (separating data which the *Requestor* is *Authorized* to receive from data that will not be disclosed to the *Requestor* pursuant to the governing policy).

C. When the *Central Gateway* discloses *Registration Data* to the *Requestor.*[28]

D. When the *Central Gateway* discards the *Registration Data* that was obtained from the *Contracted Party.* The *Central Gateway* does not retain gTLD *Registration Data*.

As discussed in the foregoing, the processing activities described in B, C and D might each be based upon legitimate interests of the *Central Gateway* operator (Art. 6 (1) f) GDPR).

[27] See Question 2, Section 8, and accompanying footnote.

[28] A *Requestor*'s collection of data from the *Central Gateway* would also be a processing activity that could be viewed as either separate from the activity of the *Central Gateway*'s disclosure to the *Requestor* or, alternatively, as part of a single processing activity/transaction.In either event, both parties must have an appropriate legal basis for this processing for such processing to be lawful under the GDPR.

Data security measures will be applied throughout the process.[29] These measures may include encryption, accountability and transparency standards, safeguards for both data subjects and *Requestors*, as well as the possibility of reviews[30] or audits.

The UAM will be distributed globally with each *Contracted Party* and *Requestor* around the world. Assuming guidance received from the DPAs suggests a UAM that centralizes responsibilities associated with the disclosure of personal data contained in gTLD registration data is legally possible, issues associated with international data transfers safeguards will be appropriately considered and addressed. Consideration would also be given to the location of the *Central Gateway*.

7 Key Assumption and Underlying Conditions

As noted above, this proposed UAM builds on TSG01. While TSG01 explicitly limited itself to answering technical questions and left open policy choices, this proposed UAM makes one central assumption and assumes other underlying conditions should the model be implemented.

The central assumption is that it would be legally compliant under the GDPR to create a system, the UAM, that centralizes decision-making responsibility for the disclosure of nonpublic registration data. This UAM, with responsibilities clearly allocated to the entities within the Centralized System (the Gateway Operator, Identity Provider(s), and Authorization Provider(s)), would also ensure that the liability aspect is taken into account accordingly in respect to the different responsibilities that each actor bears in the system. It would remove responsibility from the *Contracted Parties* for the specific acts of (a) deciding whether or not to disclose data and (b) disclosure of non-public registration data from the centralized system to a *Requestor* and consequent liability associated with these responsibilities and attach it to the Centralized System

[29] See TSG01 Technical Model for Access to Non-Public Registration Data, System Requirements at Section 5, https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf.

[30] The EPDP Phase 2 team is considering specific requirements for responses to *Requestors*. As of 10 October 2019, the EPDP Phase 2 team was considering a requirement that "if the entity disclosing the data determines that disclosure would be in violation of applicable laws AND result in inconsistency with these policy recommendations, the entity disclosing the data must document the rationale and communicate this information to the requetor and ICANN Compliance (if requested)." See Building Block G, available at https://community.icann.org/display/EOTSFGRD/e.+Building+Blocks.

performing these functions within the UAM.[31] ICANN believes this is the only way for its *Contracted Parties* to participate in a UAM.[32]

In addition, this model also presupposes underlying conditions:

Condition 1: Contracted Parties continue to collect and store Registration Data. The proposed UAM presupposes that registration data will continue to be collected and stored by *Contracted Parties* in accordance with their agreements with ICANN org and ICANN consensus policies.

Condition 2: Central Gateway does not store Registration Data. Requests for non-public registration data processed via the proposed UAM would reach Contracted Parties, who would pass the data through the centralized system to the requestor. No registration data would be stored in the centralized system.

Condition 3: Access to public data is not impacted by the model. The proposed UAM assumes access to publicly available gTLD *Registration Data* will remain unchanged. That is, requestors would use RDAP to discover the authoritative server, query it, and obtain the public data.[33]

This UAM addresses access to non-public registration data, applying an assumption that there will be a policy to be developed by ICANN's multistakeholder community that sets forth specific access requirements that can be applied through the UAM. For example, it is expected that such a policy would describe who gets access to which *Registration Data* elements, and under what conditions, such as whether access may be time bound, as well as relevant safeguards.

Condition 4: All Contracted Parties operate an RDAP service. This UAM also assumes that all *Contracted Parties* will operate an RDAP service to participate in this UAM.

Condition 5: UAM applies only to Central Gateway requests. The UAM would only impact requests for data that are routed through the *Central Gateway*. A *Requestor*'s request for data directly from a *Contracted Party* would be beyond the scope of the UAM, such as a *Requestor* who presents a *Contracted Party* with a judicial order. The implementation of a UAM does not impact third parties' ability to request data directly from a *Contracted Party*. There are policy requirements in place that govern *Contracted Parties*' consideration of those requests.

---

[31] Regarding the application of the GDPR's principles of controllership to the actors within a UAM, the Temporary Specification acknowledged that the *Contracted Parties* are controllers with respect to the disclosure of nonpublic registration data to third parties. This paper aims to consider whether a UAM would consolidate controller-related responsibility with the entities within the *Centralized System*, comprising of the *Authorizer(s)* and *Identity Provider(s) as well as the Gateway Operator* (ICANN org). As a consequence such controller-related responsibility may be removed from the *Contracted Parties* with respect to the acts of (a) deciding whether or not to disclose nonpublic registration data to third parties and (b) disclosing nonpublic registration data to a requestor. If the DPAs would view the *Contracted Parties* as controllers *within* a UAM, ICANN org would also welcome the DPAs' views if and to what extent the parties involved would be jointly and severally liable with respect to the processing of registration data in the course of disclosing such data through a UAM.

[32] The proposed UAM is not intended or expected to impact Contracted Parties' responsibilities under the GDPR beyond the limited responsibilities for decision-making and disclosure that would be consolidated within the UAM.

[33] It is possible that queries for non-public *Registration Data* submitted through a UAM might also return publicly available *Registration Data* for a queried domain name in addition to the requested non-public data, depending on the policy recommendations of the EPDP Phase 2 team.

8 Guidance Requested

Based on the model outlined in this paper, ICANN org seeks clarification on the following questions:

1. Would a centralized and unified model ensure a higher level of protection for natural persons' personal data than a distributed system in which multiple actors make decisions about this data?
2. Would this proposed UAM centralize responsibility under the GDPR for the disclosure of personal data contained in gTLD Registration Data (i.e., make the Centralized System operator(s) primarily responsible, as opposed to individual Contracted Parties),[34] compared to a decentralized model where each Contracted Party would be responsible for directly receiving and responding to requests for disclosure?[35]
3. Are there other steps that could be taken as a matter of policy to ensure that the Centralized System operator(s) would take on full responsibility under the GDPR with respect to the disclosing of non-public Registration Data to a Requestor through the UAM?
4. Would a Central Gateway's processing of a full Registration Data set from Contracted Parties, as described in Section 5 (steps 6-9), be acceptable based on the rationale described in section 6.1 above, as opposed to having the Central Gateway only obtain the specific data fields that are relevant for the specific Requestor ?
5. Aside from the questions raised above and issues to be further looked into acknowledged in the paper, are there any considerations that should be taken into account when developing the model (for example, related to safeguards, accountability, transparency, and/or security)?

9 Next Steps and Importance of Guidance

As noted above, the goal of this dialogue is to determine whether responsibility associated with the disclosure of personal data contained in non-public *Registration Data* could be centralized through a UAM in which a single entity serves as *Central Gateway* operator, and how this could be created in a compliant manner that is beneficial for data subjects while at the same time upholds the public

[34] For instance, under a UAM, claims brought by individuals arising from the disclosure of personal data to a Requestor would be directed toward the entities within the Centralized System (the Authorizer(s), Identity Provider(s), and/or Gateway Operator) instead of the Contracted Party, because the entities within the UAM are the ones responsible for the act of disclosure to the Requestor. The act of disclosure by the Contracted Party to ICANN org, as Gateway Operator, would be a distinct act of processing. ICANN org's subsequent disclosure to the Requestor would be a separate act of processing. Since these actions are not "the same processing," the joint and several liability provisions in GDPR Article 82 would not apply. Centralizing responsibility for disclosure could also potentially simplify supervision and enforcement, to the extent that in cross-border cases, a single, centralized Gateway Operator could be subject to the clear oversight of a single lead authority.

[35] Would the Contracted Parties be required to have their own legal basis for transferring the full set of Registration Data to the Gateway Operator in order to fulfill an Authorized request? If yes, would the legitimate interest in a stable and secure domain name system always outweigh the registrant's interests, which will be secured by a disclosure procedure operated by the Central Gateway in accordance with GDPR requirements, thus enabling the Contracted Party to send the full set of data to the Gateway Operator without itself reviewing the Authorized request?

interest goals that gTLD *Registration Data* serve. In ICANN org's view, a UAM is only viable if the assumption that disclosure-related responsibility can be consolidated within a centralized system is correct.

The proposed UAM would allow for a unified approach for all parties -- data subjects, those who hold the registration data, as well as those who seek access to the data -- simplifying a process that currently is fragmented among thousands of individual *Contracted Parties* who consider requests for access to data based on individual assessments of requests and their own unique standards for disclosure of data. In proposing this approach, ICANN org is heeding the advice of the European Commission, which noted the importance of developing a model, "that applies to all registries and registrars and provides a stable, predictable, and workable method for accessing non-public gTLD registration data."[36]

A unified model would be expected to benefit the data subjects whose personal data is included in gTLD *Registration Data*. It would be easier to ensure transparency in a single, unified system for both data subjects and data protection authorities, as compared to the current fragmented situation. A system with fewer actors may be more easily secured. It could also be efficiently modified in response to adverse incidents, decisions, or court rulings. Data protection arrangements would need to be implemented to address matters including transfer safeguards, network security, data subject notice and access rights, transparency, and confidentiality.

A unified model is also expected to successfully meet the important public interest goals that legitimate access to non-public registration data serves for all parties involved. Such model will help to balance the privacy and data protection rights of registrants against the legitimate interests of the parties seeking access which might also be protected by fundamental rights.
As the European Court of Justice noted in recent judgment on Case C-507/17, "the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."[37]

The UAM outlined in this document does not presuppose the policy outcomes necessary for determining which parties may be authenticated and authorized, nor for what data fields they may acquire. However, it provides an outline for a model that could be implemented based on the community's policy choices in EPDP Phase 2. Further legal certainty from the European authorities about how such a model may be operationalized will inform the EPDP's ongoing policy discussions about what it calls a System for Standardized Access/Disclosure. As part of its discussions, the EPDP is also expected to recommend appropriate safeguards for personal data processed in such a system, such as steps to ensure data accuracy, data security, minimization, logging of requests, and mechanisms to verify *Requestors*' identities and legal bases for access to requested data. As noted in the EPDP Phase 2 team's policy principles (currently in draft form), the EPDP Phase 2 Team's objective is to provide a predictable, transparent, and accountable mechanism for access/disclosure of non-public registration data to third parties with a legitimate interest and a legal basis.[38] The EPDP Phase 2 Team also noted that compliance with the GDPR and other applicable data

[36] See https://www.icann.org/resources/pages/h/en/system/files/correspondence/odonohue-to-marby-03may19-en.pdf.
[37] See judgment in case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), 24 September 2019, at https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-09/cp190112en.pdf.
[38] The EPDP Phase 2 Team's policy principles, as noted in its draft Phase 2 initial report, are available at https://docs.google.com/document/d/1TKw8tOe0qgkXgBNLjVxb7l7tu20UF9t-/edit?ts=5d73b460.

protection legislation is intended to form the foundation of any proposed System for Standardized Access/Disclosure.

By working together, the community, Board, and ICANN org can produce a comprehensive policy that allows for lawful access to non-public registration data. Without this cooperation, today's fragmented approach will continue. A unified model will create a more predictable and consistent environment for data subjects and those with legitimate interests in seeking such data.

ICANN org appreciates the DPAs' willingness to consider these questions to ensure that this next phase of ICANN policy development delivers a solution for registration data access that meets the relevant GDPR requirements.

Appendix: Registration Directory Services Record Fields

The below table represents all the data fields in a registration record, as well as the fields that are not publicly displayed following the adoption of the Temporary Specification. Prior to the adoption of the Temporary Specification, all fields were publicly displayed in RDS. The Temporary Policy also required Contracted Parties to display either an anonymized email address or a web form to contact the registrant, administrative contact, or technical contact.

The EPDP Phase 1 policy recommended the discontinuation of the collection of the administrative contact information, and limited the technical contact information to be collected to name, phone number, and email address. These fields are shaded in gray.

RDS record field	Display?
Domain Name	Display
Registry Domain ID	Display (EPDP Phase 1 policy recommendation: Do not display)
Registrar WHOIS Server	Display
Registrar URL	Display
Updated Date	Display
Creation Date	Display
Registry Expiry Data	Display
Registrar Registration Expiration Date	Display
Registrar	Display
Registrar IANA ID	Display
Registrar Abuse Contact Email	Display
Registrar Abuse Contact Phone	Display
Reseller	Display
Domain Status(es)	Display
Registry Registrant ID	Do not display
Registrant Name	Do not display
Registrant Organization	Display (EPDP Phase 1 policy

	recommendation: Do not display)
Registrant Street	Do not display
Registrant City	Do not display
Registrant State/Province	Display
Registrant Postal Code	Do not display
Registrant Country	Display
Registrant Phone	Do not display
Registrant Phone Ext	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Registrant Fax	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Registrant Fax Ext	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Registrant Email	Anonymized email or web form
Registry Admin ID	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Admin Name	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Admin Organization	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Admin Street	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Admin City	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Admin State/Province	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Admin Postal Code	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Admin Country	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Admin Phone	Do not display (EPDP Phase 1 policy recommendation: Do not collect)

Admin Phone Ext	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Admin Fax	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Admin Fax Ext	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Admin Email	Anonymized email or web form (EPDP Phase 1 policy recommendation: Do not collect)
Registry Tech ID	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Tech Name	Do not display (EPDP Phase 1 policy recommendation: Optional to collect)
Tech Organization	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Tech Street	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Tech City	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Tech State/Province	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Tech Postal Code	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Tech Country	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Tech Phone	Do not display (EPDP Phase 1 policy recommendation: Optional to collect)
Tech Phone Ext	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Tech Fax	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Tech Fax Ext	Do not display (EPDP Phase 1 policy recommendation: Do not collect)
Tech Email	Anonymized email or web form (EPDP Phase 1 policy recommendation: Optional to collect)

Name Server	Display
Name Server	Display
DNSSEC	Display
DNSSEC	Display
URL of ICANN Whois Inaccuracy Complaint Form	Display
>>> Last update of WHOIS database	Display