DETAILS OF THE PROPOSAL

Appdetex GDPR Compliant WHOIS Model In Conformance With the Recommendations of the Expert Working Group's RDS Report

This proposal seeks to address the requirements of the GDPR by incorporating the model set forth in the next-generation Registration Directory Service (RDS) system of ICANN's Expert Working Group (EWG), which was created to better meet the needs of the evolving global Internet with greater accuracy, privacy, and accountability than the existing WHOIS gTLD directory service. The EWG was created, tasked, and mandated by the ICANN Board of Directors to solicit, incorporate, and obtain input and consensus approval from the diverse members of the greater ICANN community, across all stakeholder interests, in order to go forward with a clean-slate approach to a new RDS.

In doing so, the EWG considered, examined, and analyzed numerous potential models for a new RDS prior to making its final report. Several of those proposed models were outlined in the EWG's preliminary and final reports; and beyond those published therein, the EWG also considered and scrutinized many other variants and combinations. The EWG narrowed those models down to several likely candidates for further examination. After carefully considering the pros and cons associated with several possible models, especially the privacy concerns required to be addressed, the EWG report recommended its model as the best way of implementing the proposed RDS. The EWG model is the only model that can be presented to ICANN with community-wide examination and input, including scrutiny by and approval from members of the governmental agencies responsible for implementation of the GDPR. Inescapably, any other model that could be submitted to ICANN will only represent the narrower interests of the particular stakeholder putting it forward and will not have been disclosed to nor vetted by the varied and diverse ICANN community members such as the EWG model that "represents the culmination of an intense 15+ month period of work during which [a]diverse group of volunteers spent thousands of hours on in-depth research, considered over 2600 pages of public comments, survey responses, and research results, and participated in 19 public community consultations, 35 days of face-to-face EWG meetings, 42 EWG calls, more than 200 subteam calls, and countless input-gathering sessions with outside experts and community members."[1]

Accordingly, Appdetex, as a corporate ICANN accredited registrar, is proposing a WHOIS model that is compliant with the GDPR through conformance to the already documented, disclosed, and negotiated RDS recommendations set forth in the EWG report. The already vetted, comprehensive EWG report recommends abandoning

[1] See EWG Final Report Executive Summary.

today's WHOIS model of providing every user with the same entirely anonymous public access to (often inaccurate) gTLD registration data. Instead the EWG recommends a next generation RDS that collects, validates and discloses gTLD registration data for permissible purposes only. [2]

We request that ICANN submit the full EWG final report to the Hamilton law firm for a legal assessment of the model described therein to determine its compliance with the GDPR. If there are any deficiencies to the EWG model, the assessment should identify the elements of the model that are not in compliance so that corrective measures can be readily proposed in any supplemental filings.

For specificity, AppDetex recommends a phased approach in tackling this complex RDS restructure pursuant to the requirements of the EWG. In the first phase, AppDetex recommends only modifying the current WHOIS model for natural persons in the EU. Additional phases should include more robust requirements such as credentialing of certain parties, Privacy and Proxy accreditations, etc.

RDAP is key to the implementation of the EWG's RDS model and is now ready for implementation. As we face the GDPR deadline in May 2018 Appdetex is proposing to use the learnings from this report and structure a model based on some of its key elements. We have concentrated our work on purpose and access to create an interim model so that the GDPR deadline can be met.

In this initial approach, we are recommending modifying the current WHOIS model only for natural persons in the EU. In this model the registrant of a domain name will affirmatively identify their status as a natural person or legal person and state whether or not they are in the EU.

The registration flow will include ability to consent to the display of data or utilizing a proxy service. A publicly available domain name WHOIS record will be available for every registration but may be limited by the GDPR in the information displayed.

Once this initial model is approved by ICANN, Appdetex can start the implementation process and begin work on defining additional phases for implementation.

A. Registration Data

[2] See https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf

Registration Data consists of data collected from the registrant, generated data, registrar data and registry data. Each of these categories of data are included in the WHOIS record associated with the domain name.

B. Collection of Data

To enable registration of a domain name the RAA requires the collection of the following data elements:

Domain Name

First and last name or full legal name of registrant;

First and last name or, in the event registrant is a legal person, the title of the registrant's administrative contact, technical contact, and billing contact;

Postal address of registrant, administrative contact, technical contact, and billing contact;

Email address of registrant, administrative contact, technical contact, and billing contact;

Telephone contact for registrant, administrative contact, technical contact, and billing contact;

WHOIS information, as set forth in the WHOIS Specification;

Primary and Secondary Nameservers

i. Generated Data

In the registration flow data elements may be generated. The following is list of possible data elements:

EPP status codes – https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en

Creation Date

Updated Date

DNSSEC

Registrar Registration Date

ii. Registrar Data

Registrar data is supplied by the registrar managing the domain name registration the following is a list of the data elements:

Registrar WHOIS Server

Registrar URL

Registrar

Registrar IANA ID

Registrar Abuse Contact Email

Registrar Abuse Contact Phone

Reseller

iii. Registry Data

This is data is supplied by the registry. The following is a list of the data elements:

Registry Domain ID

Registry Registrant ID

Registry Admin ID

Registry Tech ID

The WHOIS record below is color coded for the above categories

Green – Data Collected from Registrant

Blue - Generated Data

Pink – Registrar Data

Yellow – Registry Data

Domain Name: EXAMPLE.TLD
Registry Domain ID: D1234567-TLD
Registrar WHOIS Server: whois.example-registrar.tld
Registrar URL: http://www.example-registrar.tld
Updated Date: 2009-05-29T20:13:00Z
Creation Date: 2000-10-08T00:45:00Z
Registrar Registration Expiration Date: 2010-10-08T00:44:59Z
Registrar: EXAMPLE REGISTRAR LLC
Registrar IANA ID: 5555555
Registrar Abuse Contact Email: email@registrar.tld
Registrar Abuse Contact Phone: +1.1235551234
Reseller: EXAMPLE RESELLER[1]
Domain Status: clientDeleteProhibited[2]
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Registry Registrant ID: 5372808-ERL[3]
Registrant Name: EXAMPLE REGISTRANT[4]
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP[5]
Registrant Postal Code: A1A1A1[6]
Registrant Country: AA
Registrant Phone: +1.5555551212
Registrant Phone Ext: 1234[7]
Registrant Fax: +1.5555551213
Registrant Fax Ext: 4321
Registrant Email: EMAIL@EXAMPLE.TLD
Registry Admin ID: 5372809-ERL[8]
Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION
Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1
Admin Country: AA
Admin Phone: +1.5555551212
Admin Phone Ext: 1234
Admin Fax: +1.5555551213
Admin Fax Ext: 1234
Admin Email: EMAIL@EXAMPLE.TLD
Registry Tech ID: 5372811-ERL[9]
Tech Name: EXAMPLE REGISTRANT TECHNICAL
Tech Organization: EXAMPLE REGISTRANT LLC

Tech Street: 123 EXAMPLE STREET
Tech City: ANYTOWN
Tech State/Province: AP
Tech Postal Code: A1A1A1
Tech Country: AA
Tech Phone: +1.1235551234
Tech Phone Ext: 1234
Tech Fax: +1.5555551213
Tech Fax Ext: 93
Tech Email: EMAIL@EXAMPLE.TLD
Name Server: NS01.EXAMPLE-REGISTRAR.TLD[10]
Name Server: NS02.EXAMPLE-REGISTRAR.TLD
DNSSEC: signedDelegation

The GDPR protects any information relating to an identified or identifiable natural person. To ascertain if registrant data is protected by the GDPR the registration flow must ask specific questions to make this determination.

Is the registrant an identifiable Natural Person? An identifiable natural person is "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Is the registrant a Legal Person? The GDPR does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

Is the registrant in the EU?

All the current data required for a domain name registration according to the RAA will continued to be collected in this WHOIS model. The data will be processed differently based on the registrant's response to the above questions and whether the registrant is in the EU *or* the registry/registrar's collection of the registrant's data in the context of its EU establishment.

C. **Natural Person**

If the registrant identifies as a natural person and the registry/registrar is an EU establishment, or if the registry/registrar is not an EU establishment but the registrant is

in the EU, the registration flow will direct the registrant to additional options to manage the display of the data.

- The registrant can affirmatively consent to display all the data they have provided for the registration including personal data.
  If the registrant consents to display then the full WHOIS record is displayed. This consent would be indicated by ticking a box in the registration flow
- The registrant can select the option of utilizing a proxy service to mask the personal data. The use of proxy service would be indicated by ticking a box in the registration flow. This would immediately open a text box with a thorough explanation of how to utilize a proxy service and referral to the proxy vendor's website.

  If the registrant selects the option of a utilizing a proxy service to mask the data then the proxy service information will be displayed and the registrant will agree to the terms of service of the proxy service vendor. The registrant can refuse to consent to their personal data being displayed but must adhere to the terms of service of the registrar which requires that all the data provided by registrant is accurate and up to date.

- The registrant also retains the right to withdraw consent to display data at anytime. A text box in the registration flow, as well as the registrar/registry's privacy policy, would provide more information on withdrawal of consent.

All of the above choices would be incorporated into the privacy policy and terms of service of the registrar. [3]

If registrant does not consent to either display or masking the data a minimum data set is displayed with an anonymized email address. The minimum data set includes the following:

[3] Recital 32, GDPR Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided

- Domain name
- Country of registrant
- Generated data
- Registrar data
- Registry data
- Anonymized email address (to enable the ability to contact the registrant a key component for ensuring a secure and stable internet)
  Article 4 (5)[4]

No personal data will be displayed.

Domain Name: EXAMPLE.TLD
WHOIS Server: whois.example.tld
Referral URL: http://www.example.tld
Updated Date: 2009-05-29T20:13:00Z
Creation Date: 2000-10-08T00:45:00Z
Registry Expiry Date: 2010-10-08T00:44:59Z
Sponsoring Registrar: EXAMPLE REGISTRAR LLC
Sponsoring Registrar IANA ID: 5555555
Domain Status: clientDeleteProhibited (all EPP
Name Server: NS01.EXAMPLEREGISTRAR.TLD
Name Server: NS02.EXAMPLEREGISTRAR.TLD
DNSSEC: signedDelegation
Country: France
Registrant email address: Anonymized@regisrarofrecord.com

i. Natural Person not in the EU who is registering with a registry/registrar that is not an EU establishment

All WHOIS data will be displayed publicly

ii. Legal Person

The GDPR does not apply to legal entities therefore all WHOIS data will be displayed publicly unless there is personal data included in the data collected. Legal persons should be advised of best practices of managing their WHOIS data as a legal entity. Any personal data should be anonymized.

[4] GDPR Art 4, 5 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

D. Purposes
Article 5 (1)(b)

There are many legitimate purposes for collection and access of WHOIS data. Security and stability of the internet is paramount. The WHOIS data base allows users to obtain information about the status of the domain name and the contact information of the registrant and registrar for these defined purposes. The Expert Working Group and the RDS PDP have deliberated and identified permissible purposes for accessing data. [5] These purposes align with the GAC's purpose found in the document GAC PRINCIPLES REGARDING gTLD WHOIS SERVICES March 28, 2007 and reiterated in the Abu Dhabi GAC Communique.[6]

The following is a list of purposes defined by the EWG report:

i. **Domain Name Control** - Creating, managing and monitoring a Registrant's own domain name (DN), including creating the DN, updating information about the DN, transferring the DN, renewing the DN, deleting the DN, maintaining a DN portfolio, and detecting fraudulent use of the Registrant's own contact information.

ii. **Personal Data Protection**
Identifying the accredited Privacy/Proxy Provider or Secure Protected Credential Approver associated with a DN and reporting abuse, requesting reveal, or otherwise contacting that Provider

iii. **Technical Issue Resolution -** Working to resolve technical issues associated with domain name use, including email delivery issues, DNS resolution failures, and website functional issues, by contacting technical staff responsible for handling these issues.

iv. **Domain Name Certification -**Certification Authority (CA) issuing an X.509 certificate to a subject identified by a domain name needing to confirm that the DN is registered to the certificate subject.

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

[6] GAC PRINCIPLES REGARDING gTLD WHOIS SERVICES March 28, 2007 and reiterated in the Abu Dhabi GAC Communique https://gac.icann.org/advice/communiques/public/gac-60-abu-dhabi-communique.pdf

v. **Individual Internet Use** - Identifying the organization using a domain name to instill consumer trust, or contacting that organization to raise a customer complaint to them or file a complaint about them.

vi. **Business Domain Name Purchase or Sale -** Making purchase queries about a DN, acquiring a DN from another Registrant, and enabling due diligence research.

vii. **Academic/Public- Interest DNS Research -** Academic public-interest research studies about domain names published in the RDS, including public information about the Registrant and designated contacts, the domain name's history and status, and DNs registered by a given Registrant. [7]

viii. **Legal Issues -** Investigating possible fraudulent use of a Registrant's name or address by other domain names, investigating possible trademark infringement, contacting a Registrant/Licensee's legal representative prior to taking legal action and then taking a legal action if the concern is not satisfactorily addressed. Reporting abuse to someone who can investigate and address that abuse, or contacting entities associated with a domain name during an offline criminal investigation.

ix. **Regulatory and Contractual Enforcement -** Tax authority investigation of businesses with online presence, UDRP investigation, contractual compliance investigation, and registration data escrow audits.

x. **Criminal Investigation & DNS Abuse Mitigation -** Reporting abuse to someone who can investigate and address that abuse, or contacting entities associated with a domain name during an offline criminal investigation.[8]

[7] Recital 50 The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations.

[8] Recital 19 This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council ([7]). Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.

xi. **DNS Transparency** - Querying the registration data made public by Registrants to satisfy a wide variety of needs to inform the general public

D. Access

Registrant access to their WHOIS data

Registrars/registries will, at the request of the registrant, provide the registrant with a copy of their WHOIS data, as well as information on the following: (1) the purpose of maintaining and publicly posting certain WHOIS data; (2) the categories of personal data displayed on WHOIS databases; (3) any recipients of the registrant's personal data that has not been publicly posted; (4) the period for which their WHOIS data will be stored; (5) the existence of the registrant's right to request rectification or erasure of their WHOIS data, restrict processing of this data, or object to processing of this data; (6) the right to lodge a complaint with the registrar/registry's supervisory authority; and (7) the source of any WHOIS data on the registrant that has not been directly collected from the registrant.

Requestor access to public WHOIS data

Requestor is required to register and provide a validated live email address.
If the Requestor is requesting data about a natural person WHOIS record not available in the publicly available data then they will be required to identify an allowable purpose from the list above in their request for data.

This model would adhere to the EWG report recommendations surrounding the access of data outlined below:

- Logging all access to gTLD registration data, including unauthenticated access to public data elements, to enable detection and mitigation of abuses;
- Gating access to more sensitive data elements that would only be available to requestors who applied for and were accredited to receive RDS access, at the level appropriate for each user and stated purpose; and
- Auditing both public and 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.

Requestor would agree to the Terms of Service (ToS) to make a request for data. The ToS would bind the requestor to GDPR compliant terms for the use and retention of the data.

E. Retention of Data

Registrars would comply with the current retention requirements. Time limits should be established by registrars/registries for erasure or for a periodic review of data publicly available on WHOIS databases to ensure personal data is not kept for longer than necessary.

Registrars/registries will erase a registrant's personal data from public WHOIS databases without undue delay if the registrant withdraws their consent to display this information publicly or if conditions exist such that it is no longer necessary to display the data publicly (i.e. the domain name has been deleted).[9]

[9] See Art. 17 ("Right to Erasure"). "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)."