Proposal for a model to address the General Data Protection Regulation (GDPR)

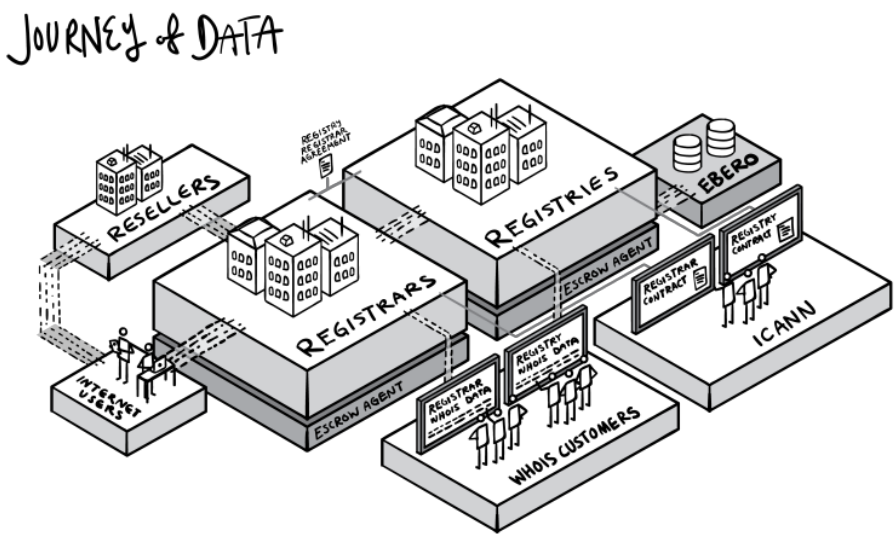
Introduction
Please find the "Executive Summary" of the data model in **Part A** of this document.

Part B responds to the requirements for a proposal published by ICANN at https://www.icann.org/resources/pages/gdpr-proposed-models-guidelines-2017-12-08-en.

For further detail on the model and explanations on the legal basis of it, we have attached the "ECO GDPR Playbook" and reference to it within the proposal.

A. Executive Summary

Key findings – Collection and "internal" processing



The data model is based on three data risk levels (DRL). These are:

- DRL 1 – Low risk – Performance of a contract (Art. 6 (1) lit. b) GDPR)
- DRL 2 – Medium risk – Legitimate interest (Art. 6 (1) lit. f) GDPR)

  The data subject has the right to object, but balancing of rights follows
- DRL 3 – High risk – Consent (Art. 6 (1) lit. a) GDPR)

  The data subject can withdraw consent at any time without any reason

Illustration 1 Illustration 2

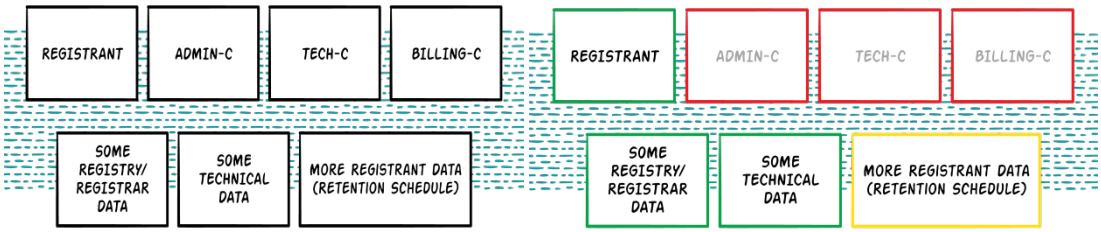
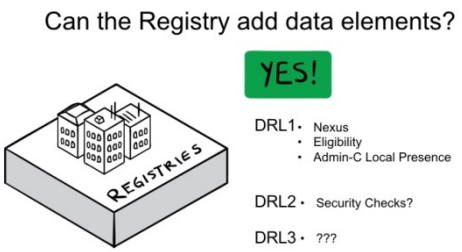


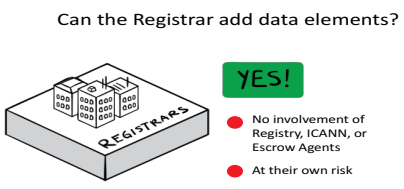
Illustration 1 shows categories of data that are required to be processed today. Much of that data is not personal. Some of the registry / registrar data can be personal data, but we trust the companies can make sure this is processed in a compliant fashion.

Registrants may be natural or legal persons. Therefore, the question arises as to whether enterprise data must be treated differently than data from private persons as registrants.
The different treatment, however, bears significant risks because enterprise names may also contain personal references and a self-identification of the registrant in this respect would not result in a reliable distribution of data inventory. In this respect, a differentiation between natural and legal persons should not be made.

Registrars: Illustration 2 shows the proposed set of data that constitutes registration data in the proposed model. Admin-C, Tech-C and Billing-C will no longer be needed. Registrant data can be collected by the registrar or their resellers in DRL1. No changes are recommended to be made to the other data elements. However, the data in the yellow box (data retention specification) shall no longer be collected based on an ICANN requirement, but according to laws applicable to the registrar or reseller.

Registries: To carry out and maintain the domain name registration, registries do not necessarily need the registrant data, but what must be discussed with DPAs is whether ICANN policy on Thick Registries can be used as a legal basis for data being stored with the registry. Apart from that, registries can specify additional requirements in the Registry Registrar Agreements according to which they can obtain data in case of nexus / eligibility requirements (DRL1) or based on legitimate interests such as security checks or reasons determined by the community in the course of the thick Whois policy development process (DRL2).





Responsibilities
For registration data, the registrar, the registry, and ICANN are joint controllers.

For data escrow, ICANN is the data controller and the escrow agents are data processors.

The EBERO is the data processor on behalf of ICANN, the data controller.

In reseller situations, the reseller is the data processor on behalf of the registrar for registration data.

Key findings - Disclosure of Data

Public Whois is not sustainable in its current form.

In order to allow for the consistent provision of information, information from different sources should be compiled by means of RDAP (delegated Whois). Furthermore, it needs to be clarified that, even at this point, registries and registrars may have more information than they provide via the Whois service.
However, disclosure, according to this paper, would only go as far as revealing the registrant data fields as currently shown in the public Whois. This means that the data of a privacy or proxy service will be shown where the registrant uses such services when gated access is provided. Disclosure by privacy or proxy services would be based on the principles applied today and remain unaffected.

There are instances in which data can be disclosed. These are:

- Disclosure to fulfill the contract (requests in conjunction with the preparation of URS and UDRP claims), Art. 6 (1) lit. b) GDPR;
- Disclosure necessary for compliance with a legal obligation to which the data controller is subject, Art. 6 (1) lit. c) GDPR (this provision serves as the legal basis for disclosure to European law enforcement agencies); and
- Disclosure based on a legitimate interest of private stakeholders, Art. 6 (1) lit. f) GDPR, see following table:

3rd Party Group	**3rd Party Interest**	**Criteria for Disclosure**	**Data to Be Disclosed**
(IPR) Attorneys Rightholders and Trademark Agents	Legal action against (IP) law infringements	• proof of admission to the bar • credible demonstration of law infringement related to a certain Domain	DRL 1
Consumer Protection Associations	Legal Action against consumer protection law infringements	• proof of entitlement to prosecution of consumer protection law infringements • credible demonstration of consumer protection law infringement related to a certain domain	DRL 1

Certification Authorities	Verification of Domain Ownership	• proof of operation of certification services (or known certification authority) • proof for request for certification by registrant	DRL 1

We should note that the limitations imposed by the GDPR will have significant impact on companies and individuals working on safety and security issues. These limitations should be discussed with DPAs with the goal of finding solutions that allow for efficient work on IT and network security.

The legal basis for disclosure to law enforcement agencies is limited to authorities acting on the grounds of EU law or national laws of EU member states.

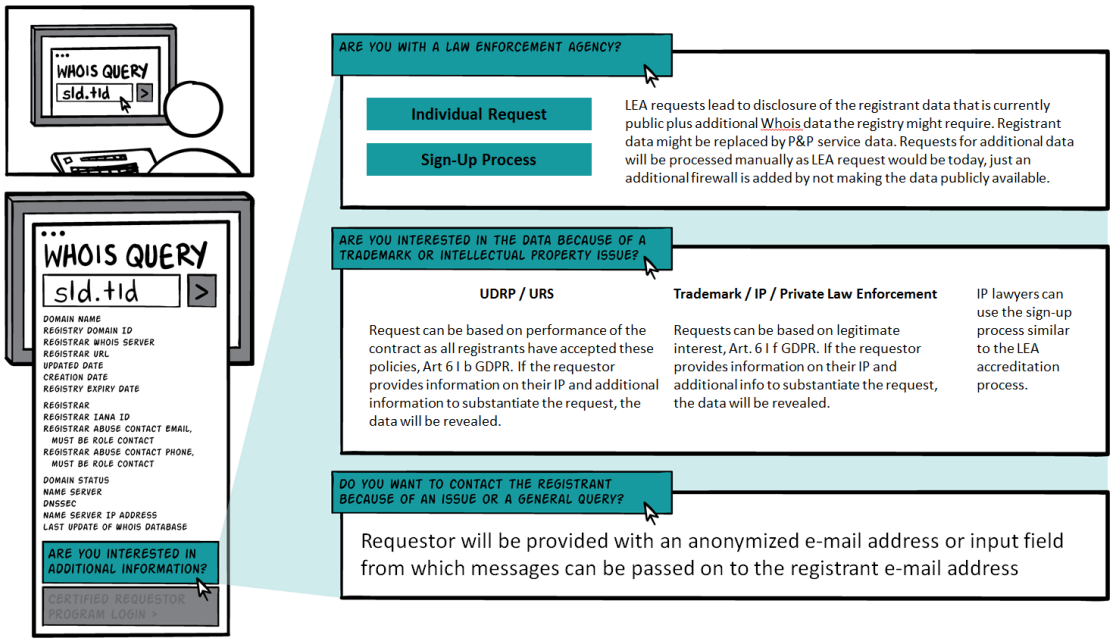
It is proposed to establish a certification program for certain user groups (public and private) and give Certified Requestors access to Whois data (which can be privacy or proxy service data) based on pre-defined criteria and limitations (such as captcha, volume limits, etc.) and only to certain data sets. Limitations could be based e.g. on the country of registrant.

It is further proposed that certification and handling of requests can be centralized in a Trusted Data Clearinghouse to avoid duplicate efforts, to remove the burden of organizational, proceduaral and financial efforts from the controllers and requesters, to ensure consistency of decision-making, and to make the system "customer friendly".

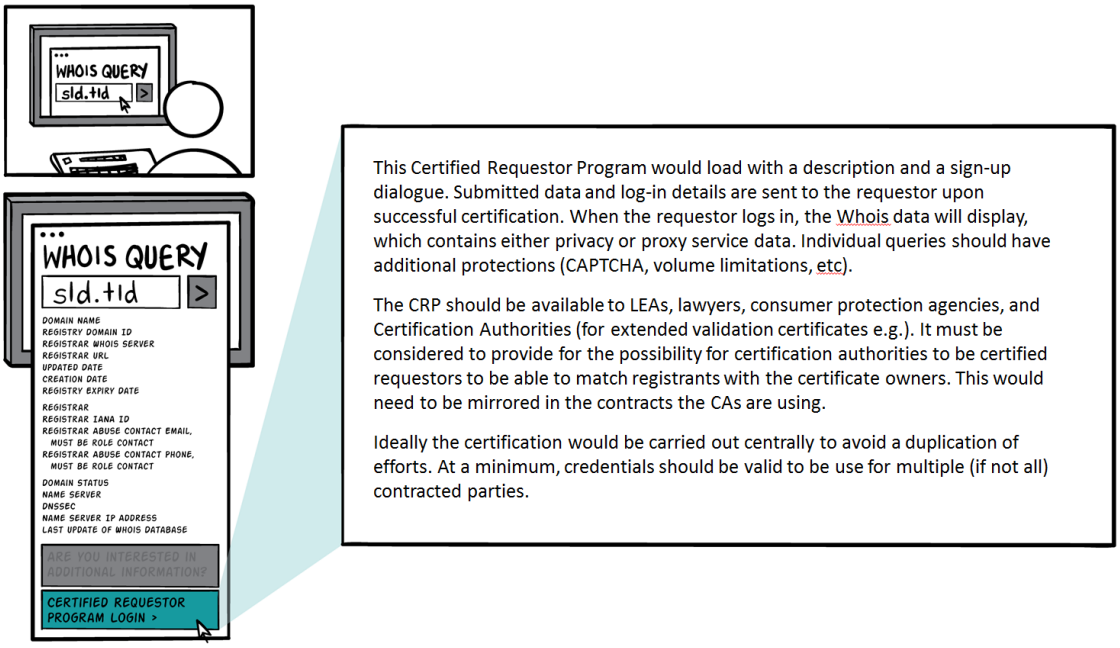
Illustration of the process: If a requestor types in a Whois query on a domain name, the Whois query will return data that comes from the registrar, including:

Domain Name
Registry Domain ID
Registrar Whois Server
Registrar URL
Updated Date
Creation Date
Registry Expiry Date
Registrar, Registrar IANA ID
Registrar Abuse Contact Email
Registrar Abuse Contact Phone
Domain Status, Name Server
DNSSEC
Name Server IP Address
Last Update of Whois Database

If a requestor is interested in further information about a registered domain, he is provided with the following options:



Certified user groups such as public authorities and third parties that can present legitimate interests can access DRL 1 data via the Certified Requestor Program:



For other general queries where disclosure cannot be justified under the GDPR, the requestor will be provided
with an anonymized e-mail address or a web form from which messages can be sent to the registrant e-mail address.

Outlook

Ideally, the contracted parties would agree on a joint data model with ICANN. The public sector also needs to be consulted and worked with, as the limited access to Whois data raises concerns. In particular, certification parameters for non-EU LEAs are an issue that should be further discussed.

Implementation of the playbook model in a timely fashion poses an additional challenge to all parties involved. Technical implementation needs to be conducted, and registry requirements need to be defined both contractually as well as in EPP. Registrars might need to waive or shorten notice periods for changes of registry requirements. It would be advisable to define different classes of registry requirements and centrally define EPP and RRA standardized language.

B. Details of the Proposal

1. Analysis of how the model accommodates existing contractual obligations while reconciling them with the GDPR, including:

a) A description of the proposed change and how it differs from the current implementation;

The model is based on the basic principle of data minimization.

DRL1

Therefore, in DRL1 only the data required for the performance of the contract is collected and processed by the contracted parties. This differs highly from the current implementation.

The registrar collects and processes less data elements as in the current situation, e.g. the data elements of Admin-C, Tech-C and Billing-C are not collected as they are not absolutely necessary for the performance of the contract.
For details on the data collected by the registrar, please refer to **Page 22** [Section II 1. a)] of the Playbook.

In addition, the registrar does transfer only a limited amount of data elements to the respective registry to minimize the data processes; regularly this is only the domain name as potential personal identifiable information according to our data model. Any additional information collected by the registrar from the registrant is not needed by the registry to perform its part of the contractual performance.
For details on the data elements transferred to the registries for their fulfillment of contractual obligations in DRL 1 please refer to **Page 28** [Section II 2. a)].

In case the registry has additional requirements (Nexus or eligibility) such can be required to be collected and transferred to the registry also for the performance of contractual obligations in DRL1, **Page 41** [Section III. 1].

DRL 2

The registry may wish to receive additional data elements which are not directly required for the registry for the performance of the contract. Such requirements must be based on legitimate interest and therefore, the registries must name legitimate purposes for the collection and/or transfer of such data by the registrar, **Page 49** [Section VII]. The Playbook lists legitimate interests that could be claimed by the registry, such as mitigating abuse, security and stability and the need for a central management. However, the list of potential legitimate interests is not exhaustive.

DRL3

Even with regard to data minimization and the data model described above, there may be a specific interest for registries to obtain (and disclose) personal data in excess to the described data sets. This is possible according to our model based on consent by the data subject, **Page 54** [Section VIII].

It should be noted that all of these possibilities of justification of data processing are equally valid. The classification in Data Risk Levels shall only emphasize the possible risk of different interpretation by the data

subject or the authority. The data elements as described in DRL1 should be commonly accepted as necessary for the contracted parties to fulfill their contractual obligations. A higher risk is involved when justifying the process with legitimate interest; not only because of the data subject´s right of objection but also because the term "legitimate interest" is very open for interpretation.

Therefore, the goal of the model is to clearly outline a basis of data processes which are clearly compliant. Other processes can be compliant as well but might need some more argumentation. The model also provides examples of possible interests for additional processes, **Page 49** [Section VII].

Disclosure
The model abandons public Whois and implements a model of layered access to data for different users such as Law Enforcement Authorities, IP-Laywers and others **Page 56** [Part C Section I]. Finally the model suggests the implementation of a Trusted Clearinghouse, **Page 75** [Part C Section V].

b) Identification of how the model impacts current ICANN contractual obligations and specification of the contract provision or policy that is impacted by the cited law;

According to the model proposed by us, only the data from DRL 1 are mandatory for the registration of a domain and must therefore be transmitted by the registrars to the registries (see answer to question 1 a).

For the registries, it is possible to continue to obtain the registrant's data on the basis of legitimate interest (see **Page 49** [Section VII]), so that a Thick-Whois-Model can also be maintained.

However, only the data from DRL 1 is required for the registration of a domain name, so that only this data should be enforced within the framework of the contractual obligations. So with regard to the registrant's data, only the domain name (which can be a personal date), see **Page 31** [Section II 2. a) aa)] is transferred from the registrar to the registry.

In addition, registries may continue to request and receive data from registrants on the basis of legitimate interest. In this respect, the transfer of the registrant's data to the registries is then also carried out for the purposes of contractual obligations / policies of ICANN.

ICANN should enforce only those contractual obligations for the parties concerned that correspond to the data from category DRL 1.

The Playbook details the flow of data and the roles and responsibilities of the parties involved. Thus, all contractual obligations relating to the processing of registration data are affected. These are the collection of data for the various contacts, transmission of data to the registry, publication of data via public Whois, escrowing data, agreements with the EBERO, the publication of zone files, reporting and transmission duties to ICANN as well as ICANN consensus policies.

c) Identification of the applicable section(s) of the GDPR;

- Art. 2, 3: Material and territorial scope
- Art. 5: Principles relating to processing of personal data
- Art. 6: Lawfulness of processing
- Art. 7: Conditions for consent
- Art. 12: Transparent information, communication and modalities for the exercise of the rights of the data subject
- Art. 13: Information to be provided where personal data are collected from the data subject

- Art. 14: Information to be provided where personal data have not been obtained from the data subject
- Art. 15: Right of access by the data subject
- Art. 16: Right to rectification
- Art. 17: Right to erasure ('right to be forgotten')
- Art. 18: Right to restriction of processing
- Art. 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing
- Art. 20: Right to data portability
- Art. 21: Right to object
- Art. 22: Automated individual decision-making, including profiling
- Art. 24: Responsibility of the controller
- Art. 25: Data protection by design and by default
- Art. 26: Joint controllers
- Art. 27: Representatives of controllers or processors not established in the Union
- Art. 28: Processor
- Art. 30: Records of processing activities
- Art. 32: Security of processing
- Art. 33: Notification of a personal data breach to the supervisory authority
- Art. 34: Communication of a personal data breach to the data subject
- Art. 35: Data protection impact assessment
- Art. 37 et seq: Data protection officer
- Art. 44 et seq: *Transfers of personal data to third countries or international organisations*
- Art. 77: Right to lodge a complaint with a supervisory authority
- Art. 82: Right to compensation and liability
- Art. 83: General conditions for imposing administrative fines
- Art. 84: Sanctions

d) A description of how this change will comply with the applicable law.

The proposed model is driven by the basic principles of GDPR, in particular the principle of data minimization and purpose limitation. The Playbook includes a legal assessment of the entire data model.

2. Changes to the collection, storage, display, transfer, and retention of data.

The Playbook explains in detail what data can be collected, stored, displayed and transferred. It also speaks to the question of data retention and ICANN's role in that regard.

3. Who will be impacted by the change and how (for example: registrants, users of WHOIS data, other contracted parties).

Registrants: The registrant is required to provide less data, in particular the naming of Admin-C, Tech-C and Billing-C is no longer necessary as a default.
The data is collected by the registrars or resellers. This data is no longer transferred automatically to the registry, but only if this is required either in the case of nexus / eligibility requirements (DRL 1) or if the registry requests the data transfer on the basis of a legitimate interest (DRL 2).

User of WHOIS data: The model abandons public WHOIS and implements a model of layered access to data for different users such as Law Enforcement Authorities, IP-Lawyers and others **Page 56** [Part C Section I] ,Page 3 and Question 5 of this proposal. Finally, the model suggests the implementation of a Trusted Clearinghouse, **Page 75** [Part C Section V].

Registrar: The registrars collect less data, in particular the data Admin-C, Tech-C and Billing-C are no longer collected. Basically, there is no automatic transfer of the registrant's data from the registrar to the registry, see the answer above to "Registrant".

Registry: In order to carry out and maintain the registration of the domain name, the registries do not require any registrant data, so that only the domain name as a potential personal date is transferred from the registrar to the registry. Apart from that, registries can specify additional requirements in the Registry Registrar Agreements, according to which they can obtain data in case of nexus / eligibility requirements (DRL1) or based on legitimate interests such as security checks (DRL2).
In addition, no more public WHOIS will be provided.

ICANN: ICANN's role will be redefined and changed, particularly with respect to enforcing contractual obligations and formally establishing that ICANN is a joint controller / data controller. ICANN must also ensure that data is only transferred to EBEROs that are compliant with GDPR.

EBERO: EBEROs must be GDPR compliant. They must adhere to the data flows according to the data model described in the Playbook.

Escrow Agents: Escrow agents must be GDPR compliant. They must adjust the format of data to be escrowed.

4. Interoperability between registry operators and registrars.

Interoperability between registry and registrar is given. All currently used data fields remain unchanged, but not all data fields will be populated. Some data fields will be populated with syntactically correct placeholder data. All handling of data that is not (potentially) personal data remains unchanged. Certain changes need to be made, particularly when it comes to transferring domain names, but the Playbook outlines how interoperability can be ensured if all parties operationalize the data model.

5. How users with a legitimate need for data will request and obtain data if it is no longer available in public WHOIS.

The model implements a model of layered access to data for different users such as Law Enforcement Authorities, IP-Lawyers and others Page 56 [Part C Section I] and Page 3 of this proposal. Finally the model suggests the implementation of a Trusted Clearinghouse, Page 75 [Part C Section V].

There are instances in which data can be disclosed. These are:

- Disclosure to fulfill the contract (requests in conjunction with the preparation of URS and UDRP claims), Art. 6 (1) lit. b) GDPR;

- Disclosure necessary for compliance with a legal obligation to which the data controller is subject, Art. 6 (1) lit. c) GDPR (this provision serves as the legal basis for disclosure to European law enforcement agencies); and
- Disclosure based on a legitimate interest of private stakeholders, Art. 6 (1) lit. f) GDPR, see following table:

3rd party group	**3rd party interest**	**Criteria for Disclosure**	**Data to be disclosed**
(IPR) Attorneys Rightholders and Trademark Agents	Legal action against (IP) law infringements	• proof of admission to the bar • credible demonstration of law infringement related to a certain Domain	DRL 1
Consumer Protection Associations	Legal Action against consumer protection law infringements	• proof of entitlement to prosecution of consumer protection law infringements • credible demonstration of consumer protection law infringement related to a certain domain	DRL 1
Certification Authorities	Verification of Domain Ownership	• proof of operation of certification services (or known certification authority) • proof for request for certification by Registrant	DRL 1

It is proposed to establish a certification program for certain user groups (public and private) and give Certified Requestors access to Whois data (which can be privacy or proxy service data) based on pre-defined criteria and limitations (such as captcha, volume limits etc) and only to certain data sets. Limitations could be based e.g. on the country of registrant.

It is further proposed that certification and handling of requests can be centralized in a Trusted Data Clearinghouse to avoid duplicate efforts, to take off the burden of organizational, proceduaral and financial efforts off the controllers and requesters, to ensure consistency of decision-making and to make the system "customer friendly".

6. Whether data handling will be uniform or if there will be variation based on things such as "natural person" vs. an organization, physical address of a point of contact, location of the registry operator or registrar, etc.

Data handling will be uniform, due to difficulties with differentiation between data.

Registrants may be natural or legal persons. Therefore, the question arises whether enterprise data must be treated differently than data from private persons as registrants. The different treatment however bears significant risks because enterprise names may also contain personal references and a self-identification of the registrant in this respect would not result in a reliable distribution of data inventory. In this respect, a differentiation between natural and legal persons should not be made.
However, input from DPAs should be sought whether a distinction could be made based on a self-identification by the registrant. Should that be deemed to be acceptable safeguard, differentiated treatment could be considered, **Page 23** [Section II 1. a) aa)].

7. Whether this model has been reviewed by a data protection authority. If so, indicate which data protection authority, when, and any details of their response.

No.

8. High-level description of any changes to other agreements beyond the Registry Agreement and Registrar Accreditation Agreement (for example: Registry-Registrar Agreement, Data Escrow Agreement, Registration Agreement, Registrar Reseller Agreement, Privacy Policies, etc.).

As described in question 1 (b), the model proposed here will fundamentally change the data available to the parties involved. In particular, registries will in principle only receive data from DRL 1, so that this model will affect almost all ICANN's contractual obligations, in particular Registry-Registrar Agreement, Data Escrow Agreement, Registry Registration Data Directory Services Consistent Labeling and Display Policy, Additional Whois Information Policy.

9. If applicable, how this differs from other models and whether you endorse any other model. If you endorse another model, please identify whether you endorse the entire model or specific sections.

N/A