GDPR
Domain Industry Playbook

V. 1.0

PLEASE NOTE A SUMMARY IS PROVIDED WITH A SEPARATE DOCUMENT

Authors:

[redacted]

*Fieldfisher Germany LLP, Hamburg, Germany, fieldfisher.com
**Rickert Rechtsanwaltsgesellschaft mbH, Bonn, Germany, rickert.net

Illustrations: Jeffery Frankenhauser, dougstudio.com

Part A - Introduction / Scope

The General Data Protection Regulation (GDPR) poses a challenge for the Registries, Registrars, Resellers, ICANN, and their contractors.

By May 25, 2018, all parties need to be compliant, which means not only that contracts need to be reviewed, but also that technical systems need to be revisited.

To date, various legal memoranda have been shared and several parties have worked on their own compliance, but no industry-wide proposal has been published that allows for a discussion of the respective roles and responsibilities of the parties involved as well as a review of data flows.

This paper shall facilitate the process of finding a commonly-adopted data model to allow for compatibility of the technical, organizational, and legal models the parties will use.

The paper is not to be construed as legal advice. All parties involved need to work on their GDPR compliance individually, which goes far beyond the topics discussed here.

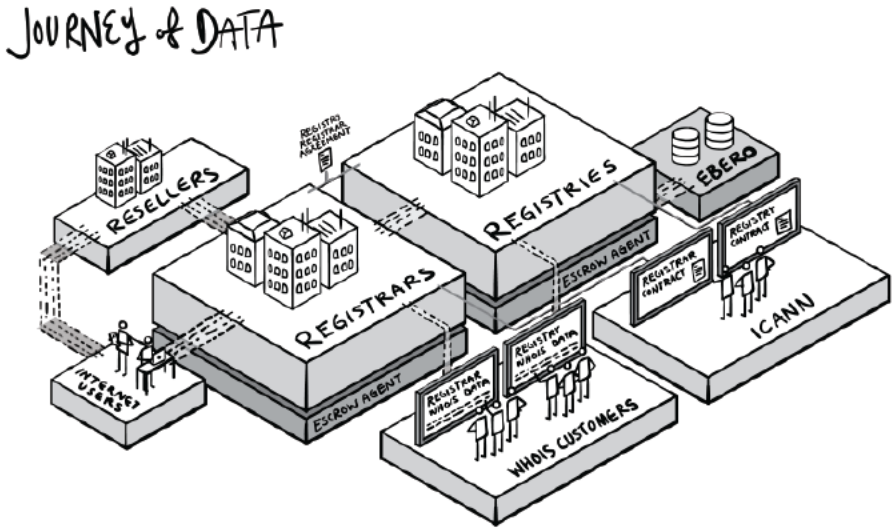
This paper only deals with the data elements which ICANN currently requires the contracted parties to process.

Furthermore, the paper will only address the data flows in the light of gTLD domain name registration services. The parties might offer additional services or wish to process additional data elements for their own business purposes. The legal basis for such processing needs to be assessed by the respective party and might lead to additional or other treatment than discussed in this paper.

The data model does not reflect any outsourcing the parties might engage in. Particular caution needs to be exercised when using a Registry Service Provider or a “Registrar as a service” model.

Data flows will be analyzed bearing in mind the parties typically involved in a domain name registration and as required by ICANN organization in its contracts. The graphic below shows how these parties are related. Dotted lines represent data flows. ICANN´s Centralized Zone Data Service (“CZDS”) and Bulk Registration Data Access (“BRDA”) have not been assessed in this papber. However, these would also

need to be reviewed. We should note that CZDS is causing concerns, as it currently enables systematic harvesting of Whois databases and leads to huge volumes of unsolicited electronic communication to registrants.



Note: This illustration includes neither outsourcing, such as RSPs or Registrar-as-a-service models, nor ICANN's CZDS and BRDA requirements.

I. Principle of Data Minimization

The RA and the RAA require the processing of numerous data elements, not all of which constitute personal data. While the GDPR only protects personal data, the paper includes all data elements, in order to allow for a holistic view of the data flows and offer a basis for implementation.

While the currently-used data records are alluded to in this paper to allow for a comparison of the status quo with the proposed data flows, the approach has not been to modify the current system by way of subtracting certain elements to achieve compliance, but rather the opposite. Based on the principle of data minimization (Art. 5 (1) lit. c) GDPR), the thought process was to start with what is required as a minimum to provide the services and to adequately recognize the rights of the data subjects, while also taking into consideration use cases and interests brought forward by law enforcement, IP interests and other groups, which are not part of the contractual relationships for gTLDs.

II. Our approach to developing a data model

The data model is based on an analysis of how data can be processed in a legally compliant fashion. Where different options for processing exist, the options with the least risk for the parties involved should be prioritized.

1. What is processing?

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (see Art. 4 no. (2) GDPR).

As can be seen from this definition, one needs to review each and every process from collection to deletion for each data element and establish what legal basis, if any, there is for processing, i.e. the processes need to be analyzed at the micro and macro levels.

To give a few examples: Data that can be legally collected by a party for a certain purpose must not be transferred to another party without a legal basis for that transfer. Data that can legally be collected and used internally must not be published without a legal basis for doing so.

2. What is lawful processing?

The GDPR offers various alternatives for lawful processing. These can be found in Art. 6 (1) GDPR, which reads as follows:

Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) 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;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

3. Risks associated with data processing

In the present case, subparagraphs

(a) Consent
(b) Performance of a contract and
(f) Legitimate Interest

of Art. 6 (1) GDPR could be applicable. The legal assessments available have provided more details on this topic, so rather than reiterating their reasoning here, we will simply base our work on those three alternatives.

It should be noted, that Art. 6 (1) lit. b) GDPR cannot be used as a legitimization for the current setup arguing that ICANN requires Registries and Registrars to collect and retain all data in their contracts. This argument would comprise of circular reasoning. What needs to be reviewed is whether the requirements ICANN presents are compliant with GDPR´s basic principles of data minimization and purpose limitation.

An analysis of the three alternatives shows that there are different risks and risk levels associated with each alternative.

a) Consent

With respect to consent, there are several factors to consider (see Art. 7 GDPR):

- The controller must be able to demonstrate that the data subject has consented.
- If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding (Art. 7 (2) GDPR).
- Consent can be withdrawn at any time without giving a reason.

[1] Hamilton October 2017 Memorandum: https://www.icann.org/en/system/files/files/gdpr-memorandum-part1-16oct17-en.pdf; [redacted]: https://www.icann.org/en/system/files/correspondence/sheckler-to-swinehart-atallah-29oct17-en.pdf; WSGR: https://gnso.icann.org/en/drafts/wsgr-icann-memorandum-25sep17-en.pdf

- Consent must be given freely. There is a prohibition of coupling.

There are risks associated with proof, such as potentially coupling consent with a domain name registration and withdrawal.

b) Legitimate interest

For data processing according to Art. 6 (1) f GDPR, there is the risk of objection according to Art. 21 (1) GDPR, which reads:

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6 (1) GDPR, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

c) Performance of a contract

There is neither a possibility of an objection, nor can any consent be withdrawn.

In summary:

- the least risk is involved with data processing required to perform a contract;
- the second best option is data processing claiming a legitimate interest, should there be any, as this gives the data controller a right to defend its position;
- the highest risk is involved with consent, as the withdrawal must be accepted by the data controller.

NOTE: When reference is made to performance of a contract in this paper, this means performance of the contract with the registrant, not e.g. contractual requirements in the contracts with ICANN.

4. Compliance requirements

ICANN has published a statement on Nov. 2nd explaining that ICANN Contractual Compliance will defer taking action against any registry or registrar for noncompliance with contractual obligations related to the handling of registration data, see https://www.icann.org/resources/pages/contractual-compliance-statement-2017-11-02-en.

ICANN also indicated that guidance on the process and eligibility criteria will be provided shortly.

In the absence of any guidance at the time of drafting of this paper, we assume that

- ICANN Contractual Compliance will not only defer taking action based on noncompliance related to registration data, but with respect to any personal data subject to GDPR. This paper refers to all personal data, and such an approach should not cause issues with ICANN Contractual Compliance.

- ICANN will support the approach taken in this paper, which is not to limit the legal assessment of data processing to only one legal basis, but instead to support a model allowing for best possible risk mitigation and compliance.

5. A layered model

Based on the above findings, the data model described in this paper will be based on three data risk levels (DRL). Minimizing the risk for all parties involved is necessary not only to avoid sanctions by authorities, but also to ensure that domain name registrations can be upheld and to limit the risk that data elements must be removed from systems operated by different parties. The levels are:

DRL 1 Low risk Performance of a contract
DRL 2 Medium risk Legitimate interest
DRL 3 High risk - Consent

As a first step, it needs to be established what data is necessary for registries to register and resolve domain names ("Registry Minimum Data record"), as well as what minimum set of data is necessary for registrars to complete the domain name registration process ("Registrar Minimum Data record"). That data falls into DRL1.

Please note that these data records may vary based on the requirements, particularly those of the registries. To give just one example: Some registries have nexus or other eligibility requirements, while others do not. However, such data would still fall into DRL1, as it is required to perform the contract.

Any additional processing, such as the transfer of data to an Escrow Agent for backup purposes, falls into the DRL1 category as defined in this paper.

As a second step, we will analyze what processing can be based on a legitimate interest. This is particularly relevant to the question of whether or not to disclose / publish data via Whois.

Since processing based on consent bears a high risk for the parties involved, and may not even be possible for certain types of processing, the model described in this paper will not include any suggestions for consent-based processing. While it is possible that parties involved will introduce such processing, consent-based processing should not be mandatorily required by ICANN due to its associated risks.

In this document, you will find a description of the journey of the various data elements.

The data in question is a subset of the data elements currently required to be processed by ICANN contracts and policies.

Contained in the document, you will find a proposal for DRL1, DRL2 and DRL3 data, as well as information on the roles of the parties, e.g. who is data processor and who is data controller? This information is required to enable the parties involved to inform the data subjects accordingly and to thereby fulfill information and transparency requirements.

We will explain why we think the solution offered is defendable. However, we do not claim that the solution offered is the only conceivable option.

It is important to note that we recommend a data model based on DRL1 to be enforced by ICANN. The recommendation arises because we do not think it is appropriate to contractually require (and sanction in case of non-compliance) contracted parties to take additional risks in the course of managing domain name registrations and their use. However, this does not mean that we are advocating against data processing according to DRL2 and DRL3. All legal grounds mentioned in the GDPR can be used for data processing (with the caveat that they are applied in a compliant manner). The data model is designed to be sufficiently open to allow for additional data processing, particularly based on legitimate interests which a party or parties involved might have. In this paper, we list several cases where a legitimate interest can be claimed to be present, but that list is not exhaustive.

The solution offered will be open for comment and consultation. It could be used on an "as-is" basis for the interim phase until such time as the policy development process to reflect the GDPR is completed. Ideally, it would be used as the basis for a long-term solution for a compliant gTLD eco-system.

6. International transfers

Please note that this paper does not elaborate on international data transfers and the safeguards that must be in place for those to be legal. For example, using EU model clauses or Privacy Shield does not make the processing of data compliant in general, and the processing described in this paper does not render the requirement for safeguards to cover international transfers redundant.

In other words: Wherever data is transferred outside the EU, that needs to be looked at both when it comes to data transfers between registrants, resellers, registrars, registries, escrow agents, the EBERO and ICANN, and also when it comes to disclosure requests where the requestor is based outside the EU.

Part B – Processing of data for domain registrations and maintaining domain registrations

I. Registration and management of the domain name

The first step (see table below) indicates the data required by the various participants in registering and maintaining a domain to comply with their contractual obligations.

1. Current data records

In its contracts and policies, ICANN specifies the data to be collected and provided by participants. The illustration below shows the corresponding relevant data.[2]

Please note that no differentiation is made here as between the specific data to be collected and provided by each participant.

All data elements currently required
Domain Name
Registry Domain ID
Registrar Whois Server
Registrar URL
Updated Date
Creation Date
Registry Expiry Date
Registrar Registration Expiration Date
Registrar
Registrar IANA ID
Registrar Abuse Contact Email
Registrar Abuse Contact Phone
Reseller
Domain Status
Registry Registrant ID

[2] https://www.icann.org/en/system/files/files/draft-gdpr-dataflow-template-registration-data-elements-29jun17-en.pdf

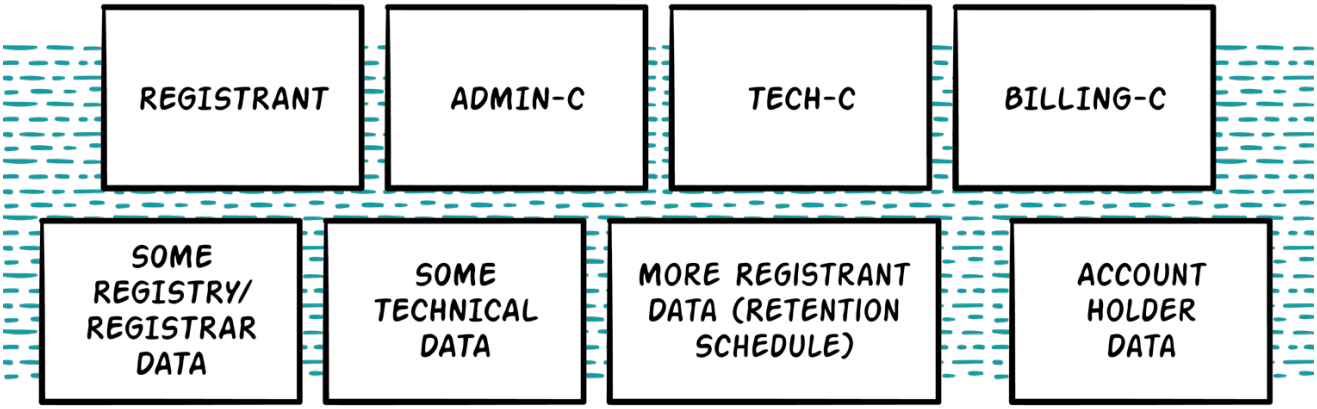
Registrant Fields • Name • Organization (opt.) • Street • City • State/province • Postal code • Country • Phone • Phone ext (opt.) • Fax (opt.) • Fax ext (opt.) • Email
2nd Email address
Admin ID
Admin Fields • Name • Organization (opt.) • Street • City • State/province • Postal code • Country • Phone • Phone ext (opt.) • Fax (opt.) • Fax ext (opt.) • Email
Tech ID
Tech Fields • Name • Organization (opt.) • Street • City • State/province • Postal code • Country • Phone • Phone ext (opt.) • Fax (opt.) • Fax ext (opt.)

• Email
Billing ID
Billing Fields (not applicable to all registries) • Name • Organization (opt.) • Street • City • State/province • Postal code • Country • Phone • Phone ext (opt.) • Fax (opt.) • Fax ext (opt.) • Email
Name Server
DNSSEC
Name Server IP Address
Last Update of Whois Database
OTHER DATA
Transfer Contact Driver's License
Transfer Contact Passport
Transfer Contact Military ID
Transfer Contact State/Government Issued ID
Transfer Contact Birth Certificate
Registrar Primary Contact Name
Registrar Primary Contact Address
Registrar Primary Contact Phone Number
Registrar Primary Contact Fax Number
Registrar Primary Contact Email Address
Name and Contact Information of Shareholders with 5% ownership interest in Registrar
Full name, contact information, and position of all directors of the Registrar
Full name, contact information, and position of all officers of the Registrar
Ultimate parent entity of the Registrar, if applicable
List of Registrars' Resellers
Registrant IP Address

Maintainer URL
The ENS_AuthId identifying the authorization of the registration

Last Transferred Date
Name Server Status
Any other registry data that Registrar submitted to registry operator
Types of domain name services purchased for use in connection with the registration
“Card on file,” current period third party transaction number, or other recurring payment data
Information regarding the means and source of payment reasonably necessary for the Registrar to process the registration transaction, or a transaction number provided by a third party payment processor
Log files, billing records and, … other records containing communications source and destination information, including (depending on the method of transmission and without limitation): (1) Source IP address, HTTP headers, (2) the telephone, text, or fax number; and (3) email address, Skype handle, or instant messaging identifier, associated with communications between Registrar and the registrant about the registration
Log files and, … other records associated with the registration containing dates, times, and time zones of communications and sessions, including initial registration
Privacy/Proxy Customer contact information
Those objects necessary in order to offer all of the approved Registry Services

In order to further enhance understanding, the above data elements can be categorized as shown in the following illustration.



Please note that the Account Holder Data box in the graphic does not consist of data that is required to be processed by ICANN. However, Registrars do in practice set up accounts and hence they process account holder data, which is also used for invoicing and contacting customers.

We recommend that the thick registry data model not be abandoned. We have also not recommended any changes to be made to the individual data elements / fields. However, the analysis below will indicate which of the data elements mentioned above can legitimately be collected and how they can be processed. Where data elements cannot be processed, for technical reasons, the respective data fields will be populated with syntactically correct place holder data. For an example of such place holder data, please see the below example:

Registrant Name: Not displayed due to applicable data protection law

Registrant Organization: Not displayed due to applicable data protection law

Registrant Street: Not displayed due to applicable data protection law

Registrant City: Not displayed due to applicable data protection law

Registrant State/Province:

Registrant Postal Code: 0000

Registrant Country: NL

Registrant Phone: +00.0000000

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email: email@notdisclosed.local

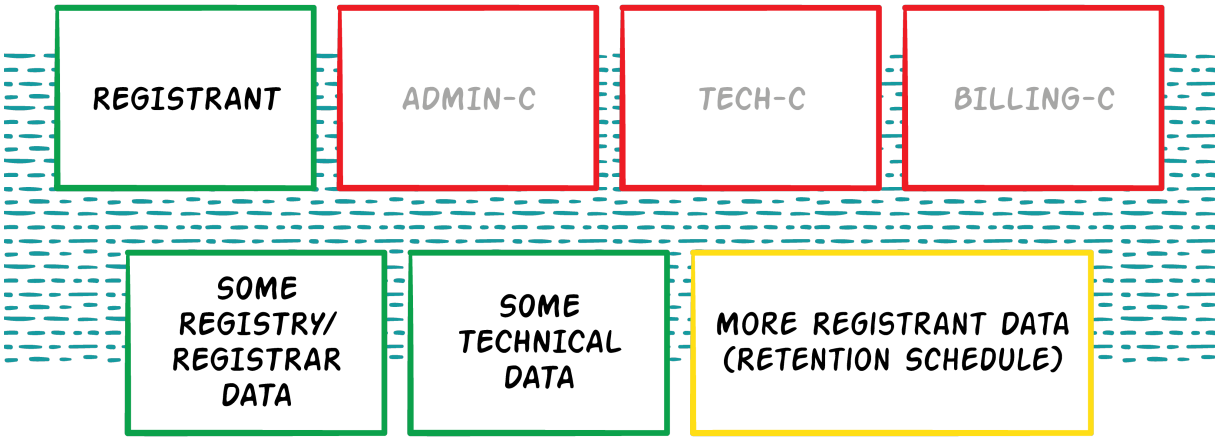
2. ICANN requirements

According to the data model proposed within this document, ICANN will and can specify the data to be collected with obligatory effect for the participants. This is the case because, while the data in category DRL1 is generally necessary for the respective participants to provide their service, it is also necessary for the stability and functionality of the overall domain system and the participants are in any case obligated by ICANN to collect and provide this data. Thus, the processing of DRL1 data shall be mandatory and enforced by ICANN.

With regard to the responsibility of the relevant participants under data protection law, reference is made to Clause II No.3 of this document.

II. DRL1 Registrar and registry data without additional eligibility/nexus criteria

All data that the various participants are obliged to collect and process for the purpose of contract fulfillment are contained in DRL1 (see Illustration below). A distinction must be made between the Registrar and the Registry, which require different data for the fulfillment of their tasks. Here, it is assumed that the registry does not have any further specific requirements for a registration.



The data elements in the red boxes are not required to be collected. The data elements in the green boxes shall be collected. Further comment on the data elements in the yellow box will be provided below.

Authorization

Art. 6 I b) GDPR allows the processing of personal data for the fulfillment or performance of a contract where the party is the contractual person. In this respect, the data mandatorily required for the fulfillment of the registration order are legitimately processed through Art. 6 I b) GDPR.

1. Registrar

a) Necessary data record – registrar

Definition of "necessary":

Processing is necessary for contract fulfillment if the contract could not be fulfilled without processing the data to the stated extent.

The registrar is the contractual partner of the registrant with regard to the registration of the domain. Within the scope of the registrant's order, the registrar will strive for registration with the relevant registry and maintain such for the registrant after successful registration.

The following data elements are obligatory for execution of the order by the registrar:

aa) Registration Data Registrar

Domain Name
Registrar Whois Server
Registrar URL
Updated Date
Creation Date
Registry Expiry Date
Registrar Registration Expiration Date
Registrar
Registrar IANA ID
Registrar Abuse Contact Email, must be role contact
Registrar Abuse Contact Phone, must be role contact
Domain Status
Registrant Fields • Name • Organization (opt.) • Street • City • State/province • Postal code • Country • Phone • Phone ext (opt.)

• Fax (opt.) • Fax ext (opt.) • Email

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 differentiated 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 as to whether a distinction could be made based on a self-identification by the registrant. Should that be deemed to be an acceptable safeguard, differentiated treatment could be considered.

From a practical standpoint, it may be desirable or even necessary to have different contact data for different purposes from the registrant. This may in particular be true for corporate customers, where it is not practical to send any communication regarding a registered domain name to one contact only and there is a need to differentiate with regard to the nature of the communication, i.e. have different contacts for technical and commercial matters. As already stated, this could also be in the registrant's own interests. Such interests for additional collection and processing of data have to be reviewed by each registrar and do not form the subject of this evaluation. Typically, these are contained in the set of data elements the registrar is processing for the customer account.

bb) Technical Data

The registrar collects the following technical data from the registrant to pass these on to the registry, so that the registry can set up domain registration on the technical side in the corresponding top-level domain namespace.

Name Server
DNSSEC
Name Server IP Address
Last Update of Whois Database

cc) Accounting Data

In addition to registration data, the registrar will also collect invoice data of the contractual partner, which is not mandatorily identical to the registrant data. The account data of the registrant or another listed obligee under the contract may also be collected and processed. This is necessary for the collection of registration and processing fees under the contract.

Furthermore, the registrar will also retain available incoming payments as well as correspondence with a registrant or contractual partner in a customer account or other customer-specific database.

This data is necessary for proper performance of the contract. As a general rule, this pertains to the following data:

• Bank data
• Customer data (insofar as different from registrant's data) • Billing data

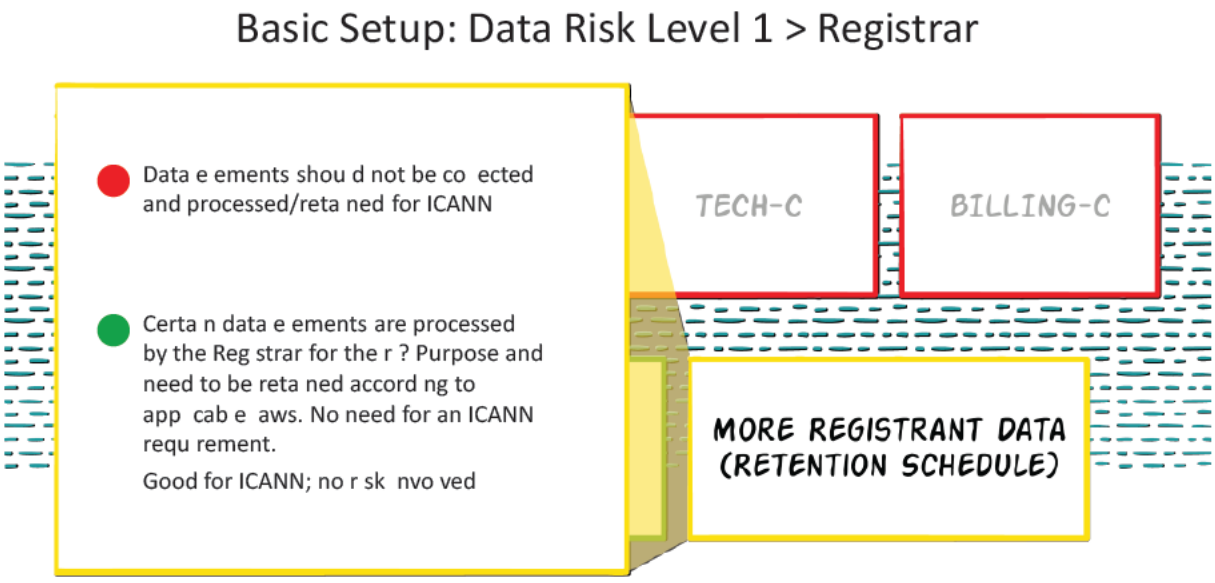
ICANN obligation

A specification by ICANN on the collection and processing of this data is not appropriate because this data is not necessary for the maintenance and stability of the DNS. Only the registrar requires the stated data for its performance of the contract vis-à-vis a contractual partner. In this respect, a compulsory specification by ICANN to store this data is not necessary to maintain the DNS. To this extent, collection and processing of the data fields following from the data retention specification should not be compulsory under ICANN. Rather, applicable statutory regulations, which should be applied, exist for the relevant registrar regarding the obligation to collect and retain data. This data may be requested from customers, so that no disadvantages should exist, e.g. for prosecution authorities in cases of legitimate collection and storage. Processing at the behest of ICANN might result in a joint controller situation (see ICANN 3 b bb (iv)), with the consequence that ICANN would bear liability risks for these data elements. This, however, does not appear to be in ICANN's best interests.

Specifically, this pertains to the following data elements:

Any other registry data that registrar submitted to registry operator

Types of domain name services purchased for use in connection with the registration
"Card on file," current period third party transaction number, or other recurring payment data
Information regarding the means and source of payment reasonably necessary for the Registrar to process the Registration transaction, or a transaction number provided by a third party payment processor
Log files, billing records and, … other records containing communications source and destination information, including, depending on the method of transmission and without limitation: (1) Source IP address, HTTP headers, (2) the telephone, text, or fax number, and (3) email address, Skype handle, or instant messaging identifier associated with communications between Registrar and the registrant about the Registration
Log files and, … other records associated with the Registration containing dates, times, and time zones of communications and sessions, including initial registration



The data in the data retention schedule may be collected and processed by registrars according to applicable legal requirements, but they should not be mandated by ICANN.

dd) Admin, Tech, and Billing Contacts

The provision of admin, tech, or billing contact data is not necessary in terms of Art. 6 (1) lit. b) GDPR, because they are not necessary to perform registration for either the registrar or the registry. The data fields currently required in this respect can be deleted without substitution.

ee) Further Data

Registrar primary contact

In light of further data retained by the registrar with regard to domain registration, the "registrar primary contact" data record recorded by the registrar itself is still relevant under data protection law. The registrar's own employee data disclosed here by the registrar itself for contact purposes is necessary for fulfillment of the contract, in order to offer the registrant the opportunity for contact within the scope of the contract.

b) Reasons

aa) Contract processing

The registrar must be able to allocate a specific domain to a specific customer in order to manage and process its internal contract handling. In this respect, the registrar must be allowed to allocate the domains registered through its service to specific customers, in order to be in a position to allocate and implement inquiries and requests within the scope of domain management to the actual owner or authorized person.

bb) Contacting / Transfer issues

The registrar must furthermore be able to contact its customers within the scope of current contracts. With respect to domain registrations, a quick and easy access to registrants is also necessary to be able to address any problems or other anomalies with regard to the domain name which may arise.[3]

The current procedure for domain name transfers via email communication cannot be continued due to GDPR requirements. At present, emails can be sent to the Admin-C to get transfers confirmed. In the absence of collection of Admin-C data, the transfer process needs to be revised. Furthermore, as Part C of this document will explain, the registrant's email address will no longer be published.
We therefore suggest establishing a new system based on secure auth-codes with the option of revoking transfers within a reasonable timeframe. As such, the disclosure of the registrant´s email address in a public Whois is no longer required. This way, the principle of data minimization is fulfilled.

[3] Overall in this respect see https://www.icann.org/resources/pages/gtld-registration-dataflow-matrix-2017-07-24-en

Alternatively, transfers can still be carried out without having an email address published by means of communication between the registrars. Since the Inter Registrar Transfer Policy allows for contacting either the registrant or the Admin-C email address, it would need to be clarified that only the registrant email address must be used for transfers.

We should note that registrars are currently engaged in discussions about new ways to facilitate transfers, and these discussions could contribute to a solution. What's more, a distinction needs to be made between transfers and trades (owner changes), as these have different legal and operational implications.

cc) Abuse

This category may refer to cases in which the domain is abused externally by third parties or to cases in which it is suspected that the registrant itself is involved in performing an act of infringement. The registrar must also be able to fulfill legitimate claims of third parties with regard to the domain or the relevant registrant. In this respect, a need to quickly establish contact with the customer frequently arises.

dd) Ownership position

The registrar has an interest in quickly and directly contacting the registrant in case of disputes concerning factual and legitimate ownership of the registrant with regard to the domain and/or to have ownership confirmed by the listed owner.

ee) Transfers

Even in the event of a transfer to another registrar and inquiries or requests received in this respect, it may be in the registrar's (and registrant's) interest if the registrar in case of doubt can quickly contact the registrant.

ff) Result

For this part of domain management, it is correspondingly necessary for the registrar to collect and store the registrant's full contact data.

Unfeasible domain registration

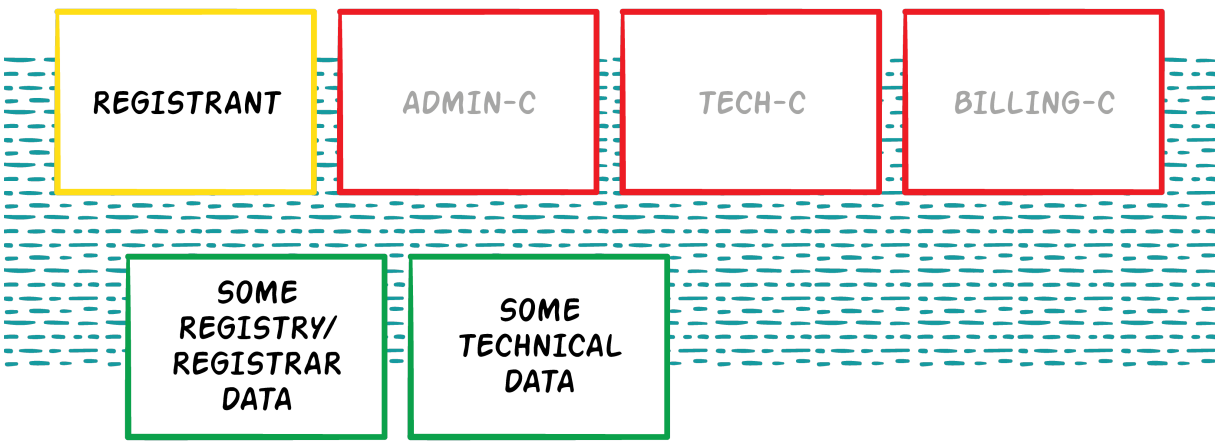
Since the registrar has no guarantee that a registration can in fact be performed by the registry, it may occur that the registrar has already collected the registrant's data but that a domain is ultimately not registered.

In this case, data collection may be justified even if a registration can ultimately not be executed, because the justification pursuant to Art. 6 I b) GDPR also encapsulates pre-contractual measures. Furthermore, the registrar's effort to register represents the content of the order vis-à-vis the registrant, so that contract fulfillment measures exist with regard to fulfillment of this contract, but not pre-contractual measures.

2. Registry

a) Necessary data record – registry

Through the relevant RRA, the registry is the registrar's contractual partner and responsible for the technical implementation of domain registrations and their maintenance. In the process, the registry reviews the availability of a domain name, registration of a domain name, and subsequently the technical availability of the domain name through the DNS.



The following data is compulsory for the registry to perform registration and to maintain the same, and must be collected by the registrar and transferred to the registry:

	Registration Data - Registry
	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, must be role contact
	Registrar Abuse Contact Phone, must be role contact
	Domain Status

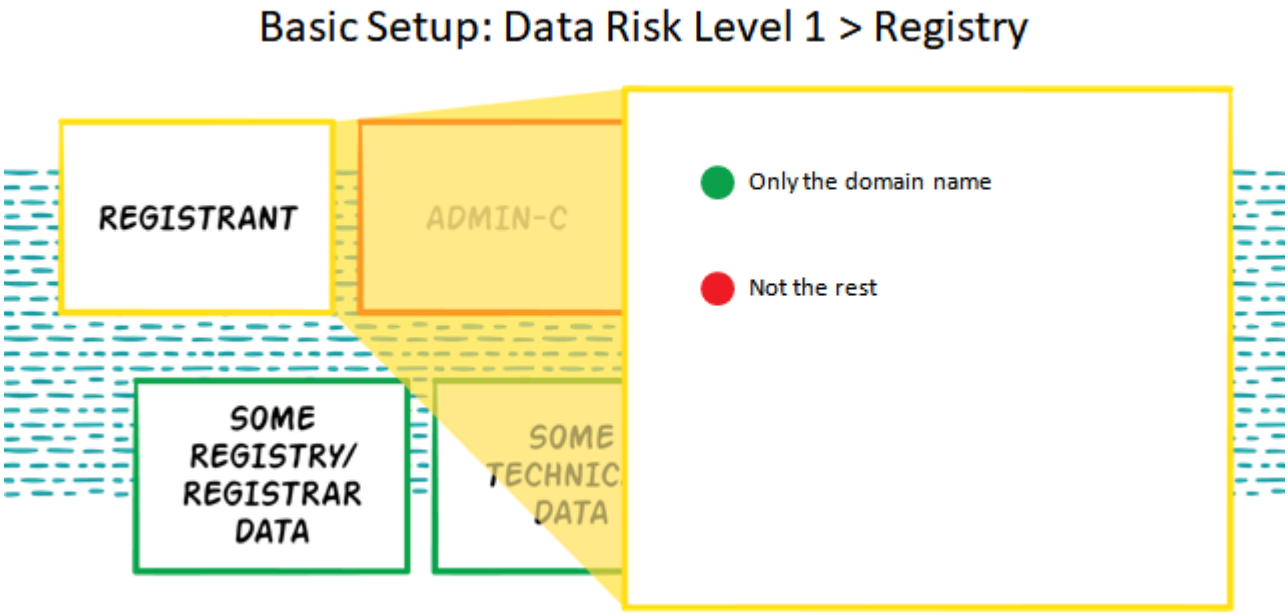
From a data protection perspective, only the domain name is relevant for the registry as potentially involving personal data.

However, a policy development process involving all ICANN stakeholders has confirmed by way of a consensus policy that is binding for all contracted parties, that a thick Whois model should be maintained by all registries. The logic behind this embraces archival and restoration purposes as well as the objective of improving data quality. We are seeking input from the DPAs as to whether such a policy can be used as a justification for the transfer of registrant data from the registrar to the registry and for such a requirement to be enforceable by ICANN. That does not mean that such data should be available via a public Whois service.

The same applies to technical data which is required for the registry to perform registration and to maintain the connection:

Name Server
DNSSEC
Name Server IP Address
Last Update of Whois Database

The remaining data, in particular the data pertaining to the registrar, does not constitute data that is identifiable or that pertains to an identified natural person. As such, this data is currently not relevant under data protection law.



aa) Qualification of the domain name as personal data

A domain name may be personal data in terms of the GDPR. The differentiation process involved in determining whether the relevant domain represents personal data causes major problems in practice[4]; as such, we are considering all domain names to be personal data within the scope of this paper.

[4] See also Hamilton, December 2017 Memorandum, paragraph 2.18.2: https://www.icann.org/en/system/files/files/gdpr-memorandum-part2-18dec17-en.pdf

Pursuant to Art. 4 no. (1) GDPR, "personal data" means any information relating to an identified or identifiable natural person ("data subject"); 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.

A domain name is data that is allocated to a specific person or enterprise. As soon as the owner of a domain is a natural person, the domain name therefore constitutes data pertaining to an identifiable natural person. The fact that the identification of the registrant under the model shown here is not easily possible for the registry itself to identify has no effect on the qualification as personal data.

In this respect, the European Court of Justice (ECJ), when considering a similar case situation[5] the storage of dynamic IP addresses of visitors at websites of official authorities ruled that, with regard to the qualification as personal data, it is irrelevant that this data cannot be allocated to a natural person by the collecting or storing entity itself. Pursuant to the judgment of the ECJ, the identifiability of the person behind the data is already sufficient. With regard to the variant of an official authority storing the dynamic IP address, reference was made to the disclosure of the connection to a natural person in particular through the information processes vis-à-vis the relevant telecommunication provider.

Following this line of reasoning, a domain name is also data that in the present model can be disclosed by the registrar.
By limiting the protection of the GDPR to natural persons (see previous definition of Art. 4 no. (1) GDPR), only domain names with natural persons as registrants would be subject to the protection of the GDPR. However, this gives rise to potential allocation problems on several levels. Firstly, the registry does not know whether the registrant of a domain name is a natural or a legal person. In the present model, this disclosure is only possible for the registrar to undertake.

Even with a clear allocation of the domain name to a natural or legal person, the domain name itself may contain name components of a natural person and thus personal references. Furthermore, the protective scope of the GDPR may also be open with regard to legal persons, if and insofar as the

[5] ECJ, judgment of 19 October 2016, C-582/14

enterprise name of a legal person itself may contain name components enabling an allocation to a natural person.

It should be clarified that Recital 14 does not change this result. It has the following wording:

> *The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation 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.*

The scope of Recital 14 may still be open for interpretation. However, it is our opinion that it does not contradict the conclusions as detailed above i.e. that even the domain name of a legal person can be deemed as constituting personal data in certain cases.
Recital 14 shall not limit the protection of rights of individuals with regard to their data. Looking at a domain name registered on a legal person whose entity name is constituted by the name (or parts of it) of a natural person: it is clear that such a name can also be used to identify the person behind the entity´s name. Even though Recital 14 limits the applicability of GDPR to the legal person itself, this does not hinder the applicability and need for protection of the natural person behind the legal person. This is true in particular with regard to small legal persons consisting possibly of just one natural person.

Also, in a judgment of the ECJ of 9 November 2012, Case C-92,93/09, the Court of Justice ruled in paragraph 53 that the protection of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (hereinafter referred to as "the Charter") is in particular subject to the protection of small legal persons (one person enterprises / sole proprietorships). Article 7 and 8 of the Charter specifically protect “Respect for private and family life” and “Protection of Personal Data”, so that it can be presumed that Recital 14 relates only to data relating exclusively to legal persons and not to natural persons.

This is also covered by the view that data can have a double character. As such, data can have a connection to the legal person on the one hand, but on the other hand also a connection to the natural

person concerned, so that at least the reference point to the natural person is protected by GDPR.[6] Due to the extreme difficulties in defining the boundaries, we therefore treat all domain names as if they were personal data.

The processing of the domain name for DNS(SEC) and a public Whois is required for the execution of the contractual relationship within the scope of Art. 6 (1) lit. b) GDPR and is therefore permissible.

bb) Result

Based on these uncertainties, all domain names must be treated as if they constitute personal data in terms of GDPR. This, on the one hand, specifically circumvents potential delimitation problems, while on the other hand ensures sufficient data protection under the GDPR for each domain name. The domain names on DNS servers are equally affected by this.

b) Reasons

The authorization to process this data follows from Art. 6 (1) lit. b) GDPR, because the data are compulsory for contract fulfillment registration and allocation of the domain name to a specific IP address.

The listed data are compulsory for the registry to register and connect the domain. Registration and connection of the domain is not possible without receiving the domain name. Consequently, this also applies to maintaining the allocation of the domain as well as processing the domain name on DNS servers, the operation of which is also technically compulsory for contract fulfillment.

3. Data controller

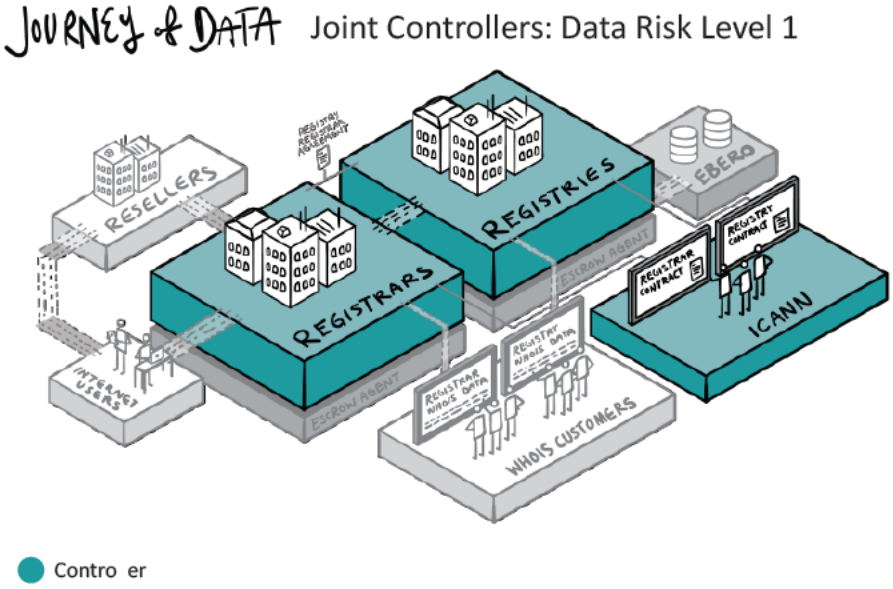
Within the scope of the suggested data model, the question arises as to who the responsible entity is for processing DRL1 registration data, in particular because only very limited data are forwarded by the registrar to the registry in order to best implement the principle of data minimization. In detail, the question arises as to whether joint or separate control exists on the side of the registrar and the registry, or whether a processor situation exists.

[6] *Paal/Pauly;* Datenschutzgrundverordnung, Art. 4, Rn. 5 f.; *Ehmann/Selmayr,* Datenschutzgrundverordnung, Art. 4, Rn. 11; *Gola,* Datenschutz-Grundverodnung, Art. 4, Rn. 22 f.

a) Definitions Art. 4 no. (7) and no. (2) GDPR

Controller is the person that alone or jointly with others determines the purpose and means of processing. Processing, in turn is "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

b) Joint responsibility (Art. 26 GDPR in conjunction with Art. 4 no. (7) GDPR)



The prerequisite for a joint responsibility of registry, registrar, and ICANN is that all jointly determine the purposes and means for processing.

aa) Hamilton opinion

The Hamilton opinion commissioned by ICANN states that, due to the complexity of processing structures, it is recommended that joint responsibility between ICANN, registrar, and registry be

assumed (October 2017 Memoradum gTLD Registration Directory Service and the GDPR, Part 1, Section 3.7.3). This also results in the most extensive liability, which also sufficiently satisfies the interests of supervisory authorities.

bb) Comment

Pursuant to Art. 4 no. (7) GDPR "controller" means the natural or legal person, public authority, agency or other body which, **alone or jointly with others**, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Art. 26 GDPR specifies the joint responsibility in terms of specifying the manner in which those jointly determining the purposes and means of processing shall be responsible ("Joint Controller"). Decision-making power concerning purpose and means of processing is decisive for determining responsibility.

(i) Distinction between processor and controller

In contrast to joint controllers, processors do not have freedom to make decisions with regard to the purposes and means of processing, but act for the contractor with a duty to comply with instructions. Insofar as the agents have options to select or design the purpose or means of processing, they are considered to be controllers jointly with the contractor and correspondingly have additional obligations.[7]

The purpose of processing is an "expected result that is intended or guides planned actions". The means of processing is the "type and manner in which a result or objective is achieved"[8].

Processors must be distinguished from joint controllers based on the following criteria:

- A person that has no legal or factual influence on the decision concerning the purposes for and manner in which personal data is processed cannot be a controller.
- A person that alone or jointly with others decides on the purposes of processing is always a controller.
- The controller may also delegate the decision concerning the means of processing to the processor as long as content-related decisions, e.g. concerning the legitimacy of processing, are reserved for the controller.

[7] *Klabunde* in *Ehmann/Selmayr* „Datenschutz-Grundverordnung" Art.4 marg. no. 29

[8] Art. 29 Data Protection Working Party, Statement 1/2010 of 16 February 2010, p. 16, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf

- Processors are independent legal persons who are different from the controller and who process data on behalf of the controller(s) without deciding on the purposes of processing.[9]

(ii) Distinction between joint and co-controller

It can also not be assumed that ICANN and the contracted parties are co-controllers for the processing of data, rather than joint controllers. A co-controllership would require two or more parties which are completely independent of one another, cooperatively working together in the processing of data but for different purposes.

As discussed below, the processing of registration data is covered by the overarching purpose of the registration of a domain name by all three parties in this process.

(iii) Purpose of Art. 26 GDPR

The regulation is to primarily serve the protection of the rights and freedoms of data subjects. [0] Specifically with regard to complex constellations, a clearer allocation of responsibilities is to be guaranteed for data subjects. In more complex role allocations, e.g. in the area of domain registration with several distribution levels, the data subject's right of access and other rights are to be guaranteed across levels.

"The definition of the term "processing" listed in Article 2 lit. b of the guideline does not exclude the option that diverse actors participate in diverse operations or sets of operations in connection with personal data. These operations can be executed simultaneously or in diverse stages. In such a complex environment it is even more important that roles and responsibilities can be easily allocated to ensure that the complexity of joint control does not result in an impractical division of responsibility that would affect the effectiveness of data protection law." [2]

Recital 79 GDPR furthermore clarifies that the regulation is to simplify monitoring by the supervisory authorities.

The factual control of the data process as well as control over external effects vis-à-vis the data subject is decisive when reviewing responsibility.

---

[9] Art. 29 Data Protection Working Party, Statement 1/2010 of 16 February 2010, p. 18, 39, 40, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf

[10] *Bertmann* in *Ehmann/Selmayr* "Datenschutz-Grundverordnung" Art. 26, marg. no. 1

[11] Art. 29 Data Protection Working Party, Statement 1/2010 of 16 February 2010, p. 27, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf

[12] Art. 29 Data Protection Working Party, Statement 1/2010 of 16 February 2010, p. 22, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf

Only the registrar appears vis-à-vis the registrant, as it coordinates the complete handling and maintenance of the registration. The registry handles technical implementation of the registration and reviews special requirements concerning registration (eligibility criteria), insofar as such exist.
Equal distribution is not necessary when allocating responsibility.

(iv) Set of operations

Furthermore, processing should not be artificially divided into smaller processing steps, but can be uniformly considered as a set of operations. In this respect, data collection, passing on to the registry, review and implementation and ongoing management of the registration can be considered as one set of "domain registration" operations, because it pursues the overall purpose of registering the domain for a new registrant.
This also applies if diverse agencies pursue different purposes within the processing chain, when engaged in the detail of smaller processing steps on a micro level. On a macro level, the same purpose is pursued overall with all small steps in the chain, so that a uniform set of operations specifically applies here (Art.29 Group WP 169, p. 25).
Differentiation is required when considering the operation of collecting and processing the data collected by the registrar from its customers in order to create an invoice, to maintain a customer account, and to manage the contractual relationship with its customers. This data fulfils another purpose that is not codetermined by the registry.

(v) Assessment

Registry, registrar, and ICANN must be assessed as joint controllers for the set of operations of domain registration (Art. 4 no. (7) GDPR). Due to the factual and legal separation between registrar and registry, a domain registration can mandatorily be performed only by both entities jointly.

In this respect, it must be assumed that registrar and registry jointly determine the purposes and means of processing that are compulsory for domain registration overall. In this respect, both are responsible for this set of operations pursuant to Art. 4 no. (7) and 26 GDPR.

This also corresponds to the legislative intent to have clear and simple regulations concerning responsibility in case of multiple participants and complex processing structures, and to prevent a splitting of responsibilities to protect the data subjects insofar as possible.

Pursuant to Article 1 Section 1.1 of the ICANN bylaws, ICANN has responsibility:

*“to ensure the stable and secure operation of the Internet's unique identifier systems as described in this Section 1.1(a) (the "**Mission**"). Specifically, ICANN:*

*(i) Coordinates the allocation and assignment of names in the root zone of the Domain Name System ("**DNS**") and coordinates the development and implementation of policies concerning the registration of second-level domain names in generic top-level domains ("**gTLDs**"). In this role, ICANN's scope is to coordinate the development and implementation of policies:*

- *For which uniform or coordinated resolution is reasonably necessary to facilitate the openness, interoperability, resilience, security and/or stability of the DNS including, with respect to gTLD registrars and registries, policies in the areas described in Annex G-1 and Annex G-2;”*

As already stated, ICANN fulfils this responsibility among other things by contractually specifying for the various participants the data which must mandatorily be collected and retained. With these legitimate provisions, ICANN specifies a purpose for the processing operation overall and thus becomes joint controller in addition to registry and registrar.

It should be noted that ICANN´s responsibility is unaffected by the fact that certain requirements have been discussed by many stakeholders or have been a community effort. Such joint discussion or drafting of certain policies of requirements do not affect ICANN´s role as the entity ultimately requiring the contracted parties to act in accordance with the policies issued by ICANN.

(vi) Legal consequence

As a legal consequence, Art. 26 GDPR references that the controllers reach a clear understanding in particular with regard to their performance of their duties under the GDPR as well as their joint control and must disclose it.

(1) Liability

The question arises as to how registry and registrar under joint control are liable for possible breaches in the processing operation.

(2) Data subject's claims

Pursuant to joint responsibility, the data subject in accordance with Art. 26 (3) GDPR may as a general rule fully assert its claims vis-à-vis all controllers, regardless of the contractual allocation.

Even with a clear distribution of the responsibility between the controllers, both are liable vis-à-vis external parties for the overall processing operation.

In this respect, Art. 82 (4) GDPR mandates joint and multiple liability for the data subject's right to compensation and supplements the liability regulations of Art. 26 (3) GDPR. The factual responsibility may be adjusted only *inter partes*. Therefore, having clear allocations between the parties is even more important *inter partes*.

(3) Fines

However, such joint and multiple liability does not apply to fines under Art. 83 (4) lit. a) GDPR. In this respect, registry and registrar are liable pursuant to their role allocation for breaches in their area or against duties under the GDPR, which were incumbent upon them within the scope of the contractual basis.

(4) Agreement

Joint controllers must furthermore specify, in a transparent form, who fulfills which duties vis-à-vis the data subjects, as well as who the contact point for data subject's rights is (Art. 26 (1) p. 2 GDPR).

However, the data subject is authorized to address any of the participating responsible agencies to assert its rights, regardless of the specification concerning competence (Art. 26 (3) GDPR).

The agreement is to regulate the specific controllers that are to fulfill the duties prescribed by GDPR. Pursuant to Recital 79 GDPR, the following must be specifically regulated in a transparent form:

- how the relations and functions of the controllers among each other are designed,
- how roles are distributed between controllers to fulfill data subject rights of registrants,
- on which controllers supervisory authorities execute supervisory and monitoring measures.

All controllers must fulfill information obligations independently from each other. However, Art. 26 GDPR suggests that multiple controllers fulfill information obligations centrally.

(5) Joint contact point

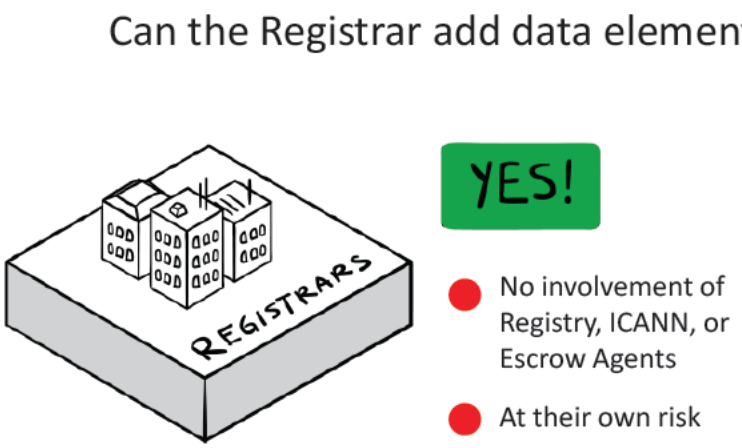
GDPR suggests that a joint contact point is set up for data subjects; however, this is not compulsory. It is suggested that this contact point is located at the registrar, because the registrar maintains contact with the registrant.

(6) Procedure record

Further, pursuant to Art. 30 GDPR, each controller must separately list its joint controllers in the record of processing activities.

cc) Responsibility for other data

Responsibility for customer data collected by the registrar merely for its own purposes lies solely with the registrar. In this respect, no joint decision is made concerning the purposes of processing. Here, only the registrar determines the purpose of processing.

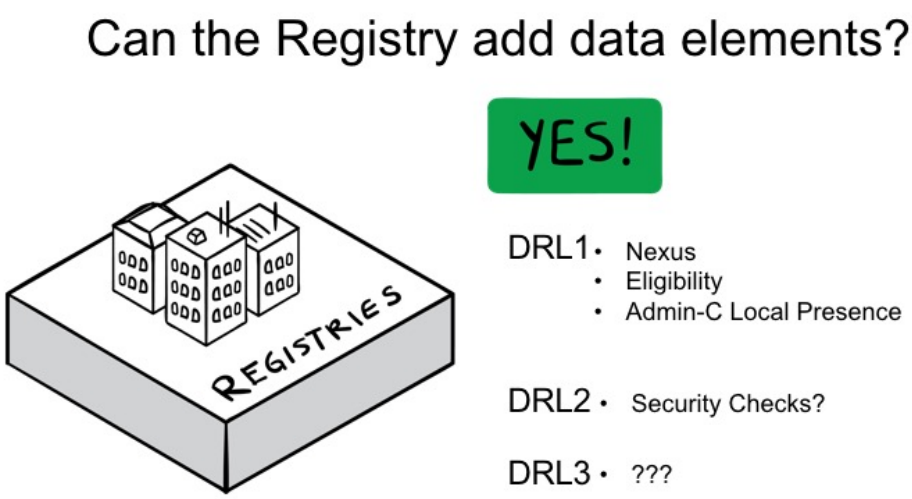


III. DRL1 registrar and registry with eligibility/nexus requirements

1. Obligation

Specific requirements that are necessary for registration under the relevant TLD (e.g. .law, .nrw, .berlin, etc.) exist. In this respect, there are TLDs with eligibility requirements (e.g. .law, .versicherung, .autos, .organic and .bank) where verification of the admission as an attorney or similar is necessary for registration authorization under the TLD, e.g. for .law/.abogado. Additionally, there are TLDs with nexus requirements (e.g. .berlin and .paris), where a geographical reference must be given for registration authorization under the relevant TLD. Today, there are more than 200 gTLDs that are marked as "restricted". In this respect, additional data is necessary for the registries in order to review

the registration authorization under these TLDs or have the validation done by a validation agent acting on their behalf.



Even more data elements which do not belong to DRL1 can be added by the registry. However, all registry requirements going beyond the minimum data set need to be explicitly spelled out in the RRA. Where no such requirement exists in the RRA, the registrar will not collect or transfer to the registry.

2. Purpose

The purpose of these additional requirements for the registration authorization is to protect the requirements of the relevant TLD system. For example, only admitted attorneys and professional legal associations (law firms, law schools, bar associations, and courts) are permitted and recognized under the eligibility requirements for the TLD ".law" and ".abogado". This creates an exclusive online space for Internet users that promotes trust in the professional legal association and offers Internet users the security of locating information on recognised attorneys and professional legal associations.

TLDs with nexus requirements create an online space for Internet users in which they can trust that the relevant offers have a geographical reference to the relevant TLD.

The purpose of the respective additional necessary data resides specifically in maintaining the exclusivity of these relevant online spaces and of offering sustainable added value to providers and users of these offers by maintaining quality.

Here, the relevant verification requirements are dependent on the respective TLD and the specific requirements of the verification. Due to the multitude of TLDs and their requirements, it is not possible here to enumerate all TLDs and their additional requirements for registration authorization in each individual case; hence, we can only offer an abstract and generalized illustration for additional requested data.

3. Responsibility

The responsibility for the additional requested data for verification of the registration authorization lies with the registry because the registry specifies the requirements concerning the relevant verification. This also applies to outsourcing of the review of requirements specified by the registry to a validation agent. Because even if the review, when using a validation agent, is not performed by the registry itself, it is in any case performed on behalf of and at the instruction of the registry vis-à-vis the validation agent. The validation agent in this respect is the processor of the registry in terms of performing the review of the verification of the registration authorization.

When collecting and transmitting the additional requested data, the registrar also acts exclusively upon instruction of the registry, so that the registrar is also processor of the registry for this additional data. The registrar does not have its own interests in these additional data or any discretion of its own concerning the purpose or means of collection and transmission of the additional requested data.

4. Authorization

The registries are authorized to demand all data required to review the registration authorization pursuant to Art. 6 (1) lit. b) GDPR.

The additional requested data is also justifiably necessary data. In comparison to the data required by ICANN for all registries, the additional data required here by the registries is justifiably required data because the respective additional required data for the relevant TLDs with eligibility/nexus requirements are required specifically to perform the registration authorization under these TLDs. In the process, these additional requirements specifically fulfill the purpose of creating an exclusive online space in which providers as well as users can profit particularly from the exclusivity of this online space and the resulting trust in the relevant offers. The requirements for additional data are therefore fully justified.

Under the principle of *data minimization* pursuant to Art. 5 (1) lit. c) GDPR, contract performance also requires a transmission of the additional data requested by the registry to the same, because this constitutes a compulsory prerequisite to review the registration authorization. It is not feasible to outsource the review of the registration authorization to the registrar in such a way as to allow the registrar to independently determine the means and purposes of the collection of the additional requirements for the registration authorization nor to undertake an independent review of the additional requirements under its own behest under data protection law, because, in this respect, it is incumbent upon the relevant registry itself to ensure the existence of the requirements demanded itself from the registration authorization.

Furthermore, in this respect it is also necessary that the registry in case of notification of a possible case of fraud is able to review the relevant authorization criteria based on the submitted documents.

IV. Data Escrow

1. Obligation

Based on Clause 3.6 of the RAA 2013, the registrar (for gTLDs) is obligated to pass on the data retained with regard to the registered domain to a neutral third-party ("escrow agent"). All data stored at the relevant registrar shall be continuously passed on. Based on Clause 2.3 of the RA in conjunction with the "specification 2" of the RA, the registry is obligated to pass its own retained data on to an escrow agent.

2. Purpose/necessity

ICANN is responsible for the security, stability, and resiliency of the DNS. To meet this responsibility, ICANN among other things imposed the stated obligations on the basis of the registry/registrar data escrow program. This is intended to specifically create a protection for registrars against loss or unavailability of the domain registration data.

3. Registrar

Data is passed on to safeguard the domain system in the event that a registrar fails due to an error, problem, or possible discontinuation of business. A loss of domain registrations or allocation problems in light of a specific domain for a certain period is to be prevented (cf. RegisterFly), because the clear allocation is also compulsory, not to mention worthy of protection for economic reasons.

The same applies to the registry data available at the registry.

4. Affected data

To fulfill the purpose of safeguarding, it is of course necessary that all registration data retained by the registrar with regard to the registered domains is transmitted to the designated third party. In the present model, the data collected and stored in DRL1 is specifically reduced to the absolute minimum quantity necessary. In this respect, logically, the transmission of all this data is also compulsory in order to achieve the purpose of safeguarding in the event of a loss. This applies equally to the data retained by the registry.

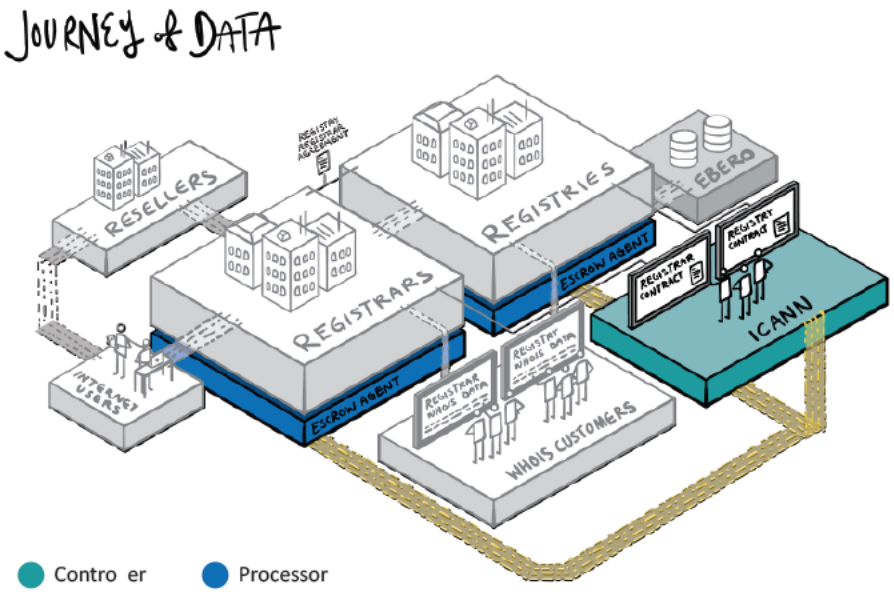
In this context, however, it is not necessary to transmit customer account data retained by a specific registrar for its customers for handling the contractual relationship to the escrow agent. In the event that a registrar fails, the retained data from the escrow agent must be transmitted to ICANN or another registrar.

5. Responsibility

As described, ICANN bears responsibility for the security, stability, and resiliency of the DNS. In this respect, ICANN determines the purpose of the processing operation “data escrow”. The registrar in this respect implements the requirements of ICANN and merely has the interest of fulfilling its own contract vis-à-vis ICANN concerning data transmission to the escrow agent, but has no real own interest with regard to security and stability of the domain system in the event of its failure. This applies equally to the registry.

With regards to registrar as well as for registry escrows, escrow agents as data controllers are therefore processors for ICANN.

It should be noted that ICANN must only pass on data received from the escrow agent to a gaining registrar or the EBERO after having verified that the gaining entity is GDPR compliant.



6. Authorization

Data forwarding to the escrow agent requires legal legitimacy. The specific requirements are deemed to be legitimate because the requirements of ICANN vis-à-vis the registrar and registry are necessary to safeguard the domain system. In this respect, data forwarding by the registrar and the registry to the escrow agents is necessary for fulfillment of the contract and justified through Art. 6 (1) b) GDPR.

V. EBERO

1. Obligation

As already stated, ICANN is responsible for security, stability, and resiliency of the DNS. ICANN wishes to meet this responsibility with EBEROs. In case of emergency events of a registry failure, EBEROs provide the backend services for the operation of a TLD originally provided by the registry.

In emergency events, the data archived by the registry at the escrow agent is transmitted to the same upon instruction by ICANN and from it to the EBERO.

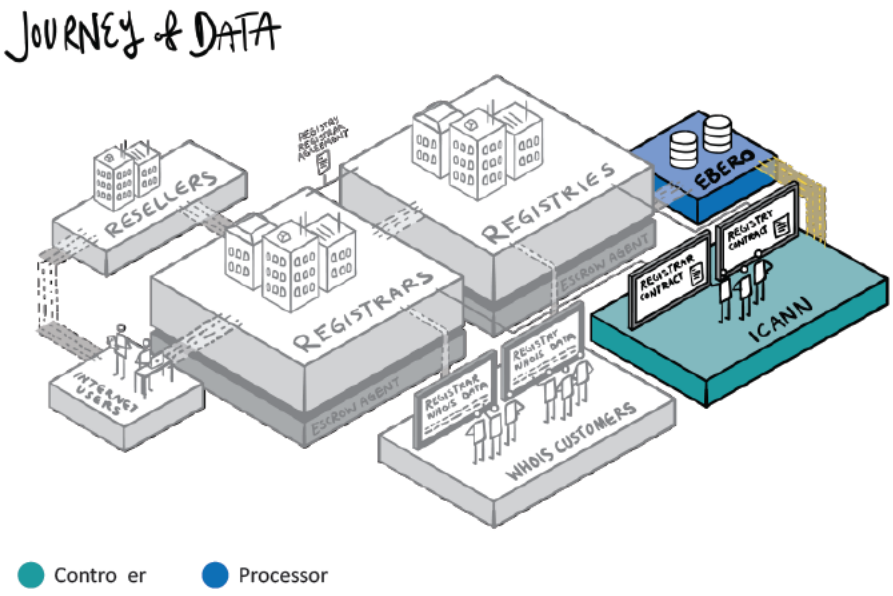
As soon as and insofar as any emergency event occurs that affects data of data subjects that is retained at the escrow service and falls under the GDPR, a GDPR-compatible EBERO is necessary.

2. Affected data

Pursuant to the data model presented here by us, the escrow agent retains only the data deposited by the registry itself (see above Part B II. 2.). To fulfill the purpose of guaranteeing the operation of the registry, it is of course necessary that all data then retained at the escrow agent is transferred through ICANN to the designated EBERO. In the suggested model, the data collected and stored in DRL1 is reduced to the absolute minimum quantity necessary. In this respect, the transfer of all this data is logically also compulsory in order to safeguard it in the event of a failure/fault.

3. Responsibility

The responsibility with regard to all data transferred to the designated EBERO lies with ICANN. The EBERO in this respect will also become active at the instruction of ICANN and does not have any discretion of its own, so that the EBERO is active as a processor of ICANN.



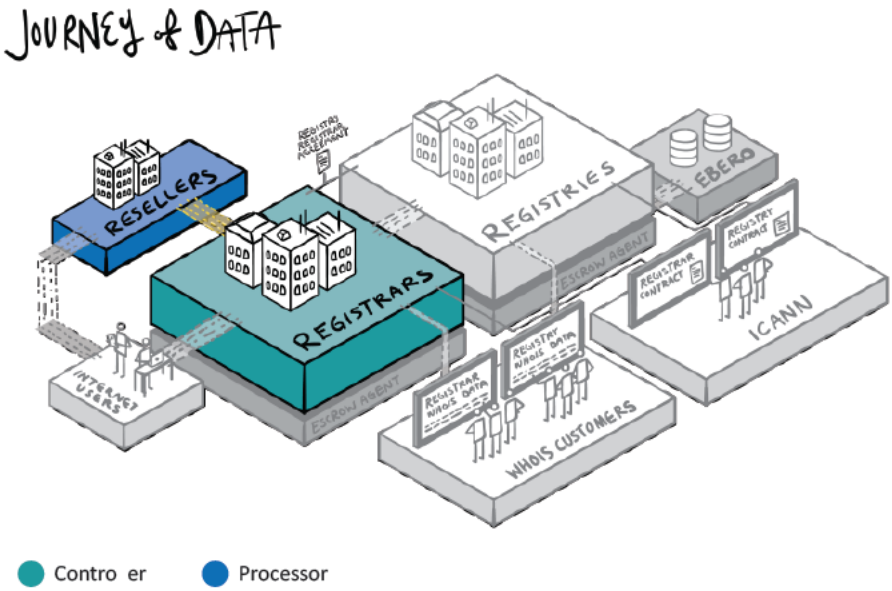
VI. Reseller situation

Insofar as the domain registration order is received by the registrar through a reseller (or a multitude of resellers), various data processing operations with various responsibilities exist.

1. Responsibility

The reseller collects the same data at the registrant that the registrar would also collect directly [3] and thus in part takes the place of the registrar. However, the reseller should not and cannot replace the registrar because only the registrar is accredited and also contractually affiliated with the relevant registries.

Accordingly, the reseller enters into the relationship with the customer instead of the registrar but cannot replace it with regard to domain registration. Therefore, it must be qualified as a processor of the registrar.



a) Account Data

In this regard, the contractual partner's account data is collected by the reseller in its own interest and for the purposes of performing its contractual relationship with the contractual partner. Accordingly, the reseller here is the sole controller for data processing.

b) Registration data

The reseller collects registration data from the registrant for the purpose of domain registration. In the process, the reseller collects solely the data necessary for registration. The relevant registry and the registrar decide upon which data is to be collected and therefore they chiefly decide on the purposes of data processing.

[13] See above Part B II. 1.

Accordingly, the registry, the registrar, and ICANN are joint controllers, even in cases where resellers are involved.

Joint responsibility with the reseller would here not be in the reseller's best interests, because the reseller does not codetermine the purpose of processing but only executes that which the other participants require in this respect.

The reseller collects this data instead of the registrar and thus on its behalf; in the process, it acts only upon the registrar's instruction and transmits the collected data for registration to it a transmission which can only be performed by the registrar. In this respect, the reseller is a processor for the registrar.

2. Reseller chains

In the event of multiple resellers in sequence, the reseller in direct contact with the registrant is the processor and the registrar is the contractor as described above. The additional resellers utilized between the two are therefore subcontractors of the respective reseller, because all parties in the chain are merely active pursuant to the original instruction of the registrar with regard to the registration data.

VII. DRL 2 – Transfer of registrant data to the registry

In the DRL2 category, as distinct from the present model for DRL1, a more extensive transmission of data from the registrar to the registry takes place. In this model, the registry might wish to receive all the registrant fields:

Registrant Fields
• Name
• Organization (opt.)
• Street
• City
• State/province
• Postal code
• Country

• Phone
• Phone ext (opt.)
• Fax (opt.)
• Fax ext (opt.)
• Email

There may be other data that the registry may claim to be able to process, based on a legitimate interest. Here, we have used the example of security checks to establish patterns of abusive / criminal behavior and stability of the DNS. The list is of course not exhaustive and can be added to on a case-by-case basis as required by the respective registry, as long as the criteria of legitimate interest are met.

1. Authorization

The data listed here are not data that are obligatory for contract fulfillment under the model suggested. A justification of this processing under Art. 6 (1) b) GDPR as data necessary for contract fulfillment is therefore not taken into consideration.
This data is thus processed based on Art. 6 (1) lit. f) GDPR.

Pursuant to Art. 6 (1) lit. f) GDPR processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The permissibility of processing therefore depends on the legitimate interests of the controller, which must take precedence in the process of balancing the data subject's protected interests.

Various purposes are considered by the registries, in which a balancing decision of the legitimate interests prevails over the protected interests of non-processing.

a) Mitigating Abuse

A legitimate interest of the registry to also receive the registrant's data listed above may follow from the fact that certain patterns at the registered domains must be received for a successful mitigation of abuse within the scope of the registration of domains. For this purpose, it may be specifically necessary

that the registry receive data of all registrants from various registrars. Otherwise, an effective abuse control could not take place, because the individual registrars could only review their own registrants' data for possible abuse. Extensive monitoring and sustainable recognition of patterns would be impossible. Pursuant to Recital 47 p. 6 GDPR, the processing of personal data to the extent that is compulsory for the prevention of fraud constitutes a justified interest of the relevant controller.

Additionally, all registries have varying legal requirements and restrictions for the registrants laid out in their Acceptable Use Policies ("AUP"). In many cases, the registries themselves are the only proper party to control and enforce compliance with the AUP under the laws of the applicable jurisdiction, as most registrars offer domain name registrations from many different registries, including many different AUP and jurisdictions.

b) Central management

The central management in terms of the equivalent to a commercial register, land register, or birth register, as well as the patent and trademark register, may also be regarded as another legitimate interest. Insofar as the registry desires the central management of the data of all registrants, this could be defined as a central management location and management of a central register. This includes the operation of a central Whois repository at the registry level (noting that the disclosure of data will occur according to the standards described in Part C of this paper).

The registry as responsible entity for the namespace operated by it can also assert a legitimate interest in the ability to allocate and identify the relevant registrants for which it provides services under its remit for the namespace. In the process, central management always also brings with it certain advantages, e.g. maintaining data accuracy in one location. Technical and organizational measures to maintain confidentiality and integrity of this data may in this case be taken by the registry itself at its own responsibility.

This also does not contradict the data minimization principle standardized in Art. 5 (1) lit. c) GDPR, because in this respect, the registry is also justified in retaining this data, based on the purpose of central management and processing of data by the registry as well. Based on its own interest for central data management, the registry also has a legitimate purpose for data processing that exceeds the purpose under DRL1.

c) *Security and stability*

The current thick whois system is based on redundancies regarding failure controls. As described above, the failure of one of the contracted parties can generally be covered by the data escrows, which is their sole purpose. However, in case a registrar fails to properly escrow its registrant data, a second fallback option for recovering this data can increase the stability and security of the domain name system immensely. If in this case the data has been transferred to the registry, it can act as a second safeguard besides the data escrow to protect the registrants.

It should be noted, that the current thick whois model has been the result of a community wide multi-stakeholder effort, via the Thick Whois Working Group, to improve the resiliency of the DNS. This community effort also included representatives of many if not all member states of the European Union via the Governmental Advisory Board and can therefore not be ignored when discussing legitimate interest.

d) *Result*

As described above, the legitimate interests described within this document are only examples of common purposes and interests that registries might have, which we believe to be generally acceptable as a legal ground for the transfer of data to the registry. This does, however, not exempt the controller, i.e. the registry, from reviewing and evaluating the legitimate interests in their individual case.

Also, although transfer of data to registries can be based on legitimate interests by the registry, these purposes and interests shall not be enforced by ICANN in their policies and requirements with the contracted parties.

2. Responsibility

The responsibility for collection and transfer of this data from the registrar to the registry lies in this case with the registry.

In this respect, the registrar is active in the collection of the previously listed data records with a dual purpose, because it receives the data for itself and its own contract fulfillment on the one hand, but on the other hand also collects this data at the instruction of the registry. The registrar therefore collects the data at its own responsibility and simultaneously as a processor for the registry.

The information obligation under Art. 14 GDPR in this respect in particular applies to the registry, because the collection of the registrants' data is not directly collected by the registry but the data is collected by the registrar and transferred to the registry.

3. Risk

In the processing of personal data based on a balancing decision under Art. 6 (1) lit. f) GDPR, the data subject is entitled to a right to object pursuant to Art. 21 GDPR. Art. 21 GDPR requires "grounds relating to his or her particular situation" from the data subject to exercise its right to object.

The requirements that are to be placed to the special situation are currently not foreseeable. However, it now already follows from the formulation "particular situation" that in comparison to other constellations, significantly higher requirements will be placed under the GDPR.

When asserting such a particular situation, the responsible entity then generally must stop processing the personal data unless it can verify compulsory grounds worthy of protection for processing, which outweigh the interests, rights, and freedoms of the data subject or serve to process the assertion, exercise, or defense of legal claims.

4. Conclusion

The collection of data by the registrar and forwarding to the registry pursuant to DRL2 takes place exclusively and to the extent as provided by the registry, subject to the justified interest in the RRA. This is to give the registrar the opportunity of reviewing the plausibility of a justified interest.

If the registry does not specify particular requirements in this respect, the registrar must stop data processing. If the registrar is of the opinion that the information concerning justified interest is not sustainable, registry and registrar must clarify this by way of negotiation. If a justified interest exists on the side of the registry, data is processed by the registrar in fulfillment of the contract with the registry, i.e. the RRA.

Under no circumstances should the processing of data be specified or enforced pursuant to this regulation by ICANN.

VIII. DRL 3 – Data collected based on consent

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, e.g. some registrants may wish to publish their data in a public Whois directory to increase trust in their services. Such special interests by registries (or other participants) can only be legitimized based on consent by the data subjects as all of the provisions mentioned above do not apply.

Such data processes are always possible in case a valid consent as required by GDPR is collected from the data subject.

Part C – Disclosure of Data

Most registries operate a so-called Thick Whois. While, from a technical point of view, this model is to be maintained, fewer data fields are populated and, unless the registry defines special requirements, the data of the registrant is also not passed on to the registry. Therefore, the question is to what recipient requests for information are to be addressed and how such requests can be answered. As already discussed, all procedures relating to the processing of personal data must comply with the principle of data minimization. Thus, a registry would only be able to provide less data in the context of a Whois service of some kind than a registrar.

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 might 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. That means that data of a privacy or proxy service will be shown where the registrant uses such services. Disclosure by privacy or proxy services would be based on the principles applied today and remain unaffected.**

In accordance with this principle, it is examined which information may be retrieved publicly or in the context of inquirers informing themselves and which information must be subjected to a separate

assessment before being released. Furthermore, we would like to point out that the term Whois is used both for the Whois protocol and the Whois data. In the context of this paper, we use the term merely with regard to the data, since, as a technical vehicle, RDAP is preferable for the provision of the data over the Whois protocol.

Given that the Whois serves as a global data base, the international transfer of data under the GDPR is of fundamental importance for many potential disclosure processes. Against this background, it is important to understand that each transfer of Whois data outside the EEA requires its own, separate legal basis in addition to the legal basis for the processing of personal data. In other words: Having a legal basis for the international data transfer does not substitute the requirement of a legal ground for the data processing itself.

Please do also note that Chapter 5 of the GDPR provides only potential legal grounds for the international transfer of data by entities like registries, registrars, private stakeholders or non-law enforcement authorities. The regulation does not apply to the processing or transferring of personal data by law enforcement agencies. [4] This is rather regulated by the European Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. [5]

The EWG final report has established a list of Whois users and their respective interests in accessing Whois data [6]. The gTLD Registration Dataflow Matrix and Information document also lists users and use cases [7], all of which have been reviewed by the drafting team of this paper. However, as outlined above, requests for information from all those user groups require a legal ground for the provider of a Whois database for disclosure. In this part of the paper, we first present that a publicly accessible whois directory cannot be justified under the upcoming GDPR (I.). In a second step, the criteria for disclosure for different purposes are to be examined (II.), followed by th analysis of the legal requirements for international data transfer (III.). After developing a procedure for handling information requests and

[14] See material scope of the GDPR according to Art. 2 (2) d.
[15] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.
[16] ICANN: EWG final report on gTLD Directory Services, p. 21.
[17] ICANN: Draft dTLD Registration Dataflow Matrix and Information.

disclosure of Whois data in practice (IV.), we finally provide a proposal for a Trusted Data Clearing House for the domain industry (V.).

I. No Justification for a Public WHOIS und GDPR

Already under the current European legal data protection framework, there are doubts as to whether or not the publication of personal data of domain owners via a publicly accessible WHOIS database is admissible. However, once the GDPR comes into effect in May 2018, it will have to be assumed that the WHOIS databases will not be able to continue to exist in their current form. [8]

1. Legally Ineffective Consent

Section 3.7.7.5, the RAA 2013 requires that the registrant must consent to the data processing also including the publication of Whois data. However, there are significant doubts as to whether such consent will still be able to be considered legally valid.

According to Art. 4 no. 11 GDPR, consent of the data subject means

> *"any **freely given**, specific, informed and unambiguous **indication of the data subject's wishes** by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*.

In addition, Art. 7 (4) GDPR further states that,

> *"when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, **the performance of a contract**, including the provision of a service, **is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.**"*

This provision prevents that data controllers withhold or offer a degraded version of service for subjects who refuse or (later) withdraw consent. Consent based on the contractual obligation (Section 3.7.7.5, the RAA 2013) will therefore not be valid.

[8] cf. Nygren/Stenbeck, gTLD Registration Directory Services and the GDPR - Part 1, p.10 ff.; Voigt/Pieper, Impact of the GDPR regarding WHOIS system, p. 3 et seqq.

2. No Justification under Statutory Law

Likewise, none of the statutory legal grounds of the GDPR is able to justify the Whois directory in its current form, in which all data is made available online to the general public.

The publication of data in a freely accessible directory is not necessary for the performance of contractual relation between the registrant and the registrar/registry so that a justification under Art. 6 (1) lit. b) GDPR is not possible.

Furthermore, contrary to what is the case for public trade mark and commercial registers, there is no specific legal basis legitimizing or even requiring the operation of a public domain directory. The coordination of internet communication and, therefore, also of domain registration has always been performed on the basis of legal relations between private individuals. This is why a public regulatory framework, which would e.g. also require a public directory, does not exist. Consequently, it cannot be argued that a public Whois can be justified under Art. 6 (1) lit. e) GDPR. The definition of public interests is also subject to legislative action, which has not taken place in relation to a publicly accessible Whois data.

Ultimately, the current public WHOIS directory will also not be able to be justified on the basis of Art. 6 (1) lit. f) GDPR. The circumstances described therein require a weighing of the interests in the respective data processing on the one hand and the interests of the data subject on the other hand on a case-by-case basis. It is true that there are a variety of reasons why certain authorities, individuals or groups of individuals have profound interest in accessing Whois data, therefore justifying disclosure (e.g. for identification of a person who has registered a certain domain) under the GDPR. [9] However, these individual interests do not justify the publication of personal data in a publicly accessible Whois directory, since the publication is not necessary for other purposes or to persons other than the holder of a legitimate interest.

[9] cf. in this regard ICANN: EWG final report on gTLD Directory Services, available at: https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf; ICANN: Draft dTLD Registration Dataflow Matrix and Information, available at: https://www.icann.org/en/system/files/files/gdpr-dataflow-matrix-whois-11sep17-en.pdf.

For these reasons, a closed Whois system which can be accessed in individual cases only (namely if disclosure can be justified under data protection law) and/or from which information is provided in individual cases will be required once the GDPR enters into effect. Compliance with the provisions of the regulation is particularly important for any provider of a Whois database, as violations such as non-justified disclosure can cause significant fines to be imposed by data protection authorities.

II. Legal Grounds for Disclosure of Registration Data to 3rd Parties

There are different groups of 3 [d] parties which may have an interest in the disclosure of registration data. Disclosure through data transfer is a type of data processing within the scope of Art. 4 no. (2) GDPR. In the context of disclosure of Whois data, Art. 6 GDPR exhaustively names the prerequisites under which the processing of personal data shall be lawful. In the relevant context here Art. 6 (1) lit. b), c) and f) GDPR are crucial. In this regard, it makes sense to distinguish between 3rd parties from the public and the private sector, respectively, as different legal grounds have to be considered.

1. Art. 6 (1) lit. b) GDPR - Performance of a Contract – (Private Sector Only)

According to Article 6 (1) lit. b) GDPR disclosure can be justified where

> *"processing is **necessary for the performance of a contract to which the data subject is party** or in order to take steps at the request of the data subject prior entering into a contract."*

The contractual basis of domain registration also contains, inter alia, provisions that subject registrants to certain conflict resolution regimes aiming to avoid and to resolve potential conflicts within the domain name registration ecosystem. Only those domain names can be registered and the registration of domain names can only be retained if there is no violation of third party rights. To the extent necessary for the assessment of possible legal conflicts related to the domain names , data processing including disclosure of personal data - can therefore be seen as being admissible under the performance of a contract clause. This especially concerns these following two programs that are included in the contractual relationship between the registrant and the registrar/registry:

- Uniform Domain Name Dispute Resolution Service for Generic Top-Level Domains (UDRP)
- Uniform Rapid Suspension System (URS)

To the extent that the disclosure of personal data is required within these procedures, in particular for the preparation of claims or inquiries by anyone who credibly demonstrates to have a legal position subject to these programs, Whois data may be disclosed on the basis of Art. 6 (1) b) GDPR.[20]

2. *Art. 6 (1) lit. c) GDPR (Public Sector Only)*

Disclosure of Whois data is further justified under Art. 6 (1) c) GDPR to the extent necessary for compliance with a legal obligation to which the controller is subject. Art. 6 (1) c) GDPR itself does not constitute a legal basis for data processing, but instead requires a legal obligation in the laws of the EU or the Member States.[2] From this, it can be inferred that legal provisions of third-party countries which have not been adopted by the EU or the relevant Member State, for example by transforming international treaties into national law, cannot trigger any legal obligation within the scope of Art. 6 (1) c) GDPR. Therefore, a disclosure requests of public authorities of non-EU states cannot be justified on the basis of Art. 6 (1) c) GDPR. Foreign authorities, however, may request personal data of EU data subjects from European law enforcement agencies. These agencies would then have to check whether there is a legal basis available that allows data to be passed on to the foreign authority.[22] Due to the global domain name system and the fact that non-European law enforcement authorities also have interests in registration data, which, at least theoretically, might also contain data of EU citizens, this constitutes a tremendous challenge to the proper design of a consistent disclosure process.

The term "legal obligations" in the meaning of Art. 6 (1) lit. c) GDPR does not necessarily require an act of parliament.[23] Different kinds of substantive law provisions can be considered as sufficient legal basis for processing of data (e.g. regulations and statutes on the basis of which public authorities such as law enforcement authorities or financial authorities are given competences or investigative rights). As a general rule, however, these statutory provisions must not fall short of the data protection level guaranteed by the GDPR; with the exception of cases where the GDPR itself provides for limitations of the relevant rights to private life and data protection arising from Art. 7 and 8 of the Charter of Fundamental Rights of the European Union. Such an option for possible limitations is provided by Art. 23 GDPR which mentions, inter alia, national and public security or the prevention, investigation,

[20] Please note that this legal assessment does not concern the question of whether such an agreement can be legally validly agreed between the parties, but relates solely to questions of European data protection law.
[2] Recitals 40 and 45.
[22] Please note that also the provisions for international data transfers apply (see below III.).
[23] The requirements for the legal basis are specified in Recital 41; with regard to the principles of Art. 5 (1) a GDPR (lawfulness, fairness and transparency), the explanations in Recital 39 are to be taken into consideration.

detection or prosecution of criminal offences and the execution of criminal penalties as well as the protection of other important objectives such as taxation matters or social security. Provisions regarding the data processing by authorities for the purpose of preventing, investigating, detecting or prosecuting criminal offences as well as for the execution of criminal penalties are regulated in Directive *(EU) 2016/680*[24]. Legal basis in this regard would be the respective rules under national laws of the member states transforming the provisions of the Directive into national law.
Art. 6 (3) GDPR provides a catalogue of criteria with regard to the proper design of the required legal basis. These criteria can be used as a guideline for the assessment of whether or not a provision satisfies the requirements for a "legal obligation" within the scope of Art. 6 (1) lit. c) GDPR.

The provision should specify

- which general conditions govern the lawfulness of processing by the controller,
- which types of data are subject to processing,
- which data subjects are concerned,
- to which entities and for what purposes the personal data may be disclosed,
- which purpose limitation the data is subject to,
- how long data may be stored and
- which processing operations and procedures may be used.

Whether and to what extent processing is necessary depends on the purpose for which data is processed. Therefore, the legal obligation must precisely specify the purpose.[25]

It is, of course, not a data controller´s obligation to review every possible legal basis for compliance with these requirements. However, the outlined standards provide valuable indications as to what standards information requests form government agencies have to meet.

For the operationalization of requests from public authorities, we recommend to check for the following formal criteria:

[24] Directive (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. This directive was passed together with the GDPR, however, it is not applicable to activities subject to Union law (Art. 2 (3) b GDPR). Since public security is not governed by Union law, the rights of data subjects may only be limited by EU provisions outside the scope of public security.
[25] Cf. Recital 41; also consider Recital 45, pursuant to which a law can also be the basis for several processing operations.

- the requesting organization or authority would have to electronically submit the request on a letterhead of its organization showing where the request for information comes from.
- the request must show which authorized representative has signed the request and how said representative can be contacted by telephone or email.
- the request must be signed.
- the legal basis must be specified from which the right to access Whois data can be inferred.
- It must be affirmed that the data will only be viewed and used in the context of the statutory competences of the respective organization or public authority.

3. Art. 6 (1) lit. f) GDPR – Legitimate Interests (Private Sector Only)

In some cases, the disclosure of Whois data may also be justified under the GDPR due to "legitimate interests". According to Art. 6 (1) f) GDPR, disclosure of data can be justified where

> *"processing **is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject** which require protection of personal data, in particular where the data subject is a child"*

With regard to the information requests from foreign authorities, there are no differences compared to the situation under Art. 6 (1) lit. c) GDPR. Disclosure of information to foreign country authorities cannot be justified. Recital 47 of the GDPR clearly states that data processing of the public sector must not be based on legitimate interests but on a legal basis under Art. 6 (1) lit. c) GDPR:

> *"Given that **it is for the legislator to provide by law for the legal basis for public authorities to process personal data**, that legal basis should not apply to the processing by public authorities in the performance of their tasks."*

Nothing different can apply to foreign authorities. Otherwise lower data protection standards would apply to foreign authorities than to authorities of the EU or EU Member states. It is up to the competent legislators to provide legal grounds for justifying disclosure of data to foreign authorities. Only within the limited scope of Article 49 (1) lit. d) GDPR, where international data transfer is necessary for important reasons of public interest, disclosure to foreign public authorities be justified under legitimate interests (see below Part C III 2).

a) "Legitimate Interests"

Hardly any indicators currently exist as to how the undefined legal term of “legitimate interest” will be interpreted by data protection authorities and courts after the entry into force of the GDPR. The regulation itself does not contain a definition of this term and provides only very few indications on which interests may be deemed to be “legitimate”. However, several references speak for the fact that a broad interpretation of the term can be assumed. Restrictions, proposed in the legislative process, have not been reflected in the final draft [26]. Recital 47 furthermore mentions customer relations and the service relationship only as examples for legitimate interests (“e.g. if the data subject is a customer of the controller or in its service”) and thus leaves a broad margin for interpretation. The character of Art. 6 (1) lit. f) GDPR as a "catchall element" also speaks for a broad understanding of the term. Against this background, all interests including factual, economic, and immaterial interests can be deemed to be “legitimate”.

The main purpose of any data processing operation in connection with domain registration is the provision of the services associated with domain registration within the scope of the contractual relation. However, the activity of the enterprise participating in domain registration cannot be reduced to this singular purpose. Rather, the registration of domains is a service, which - jointly with the services of other companies - guarantees the overall functionality of the Internet (namely conveying content available in the World Wide Web). The special roles of registrar and registry within this technical ecosystem is also reflected e.g. in the fact that they are subject to certain duties as operators of critical infrastructures .[27] The activity of registry and registrar - in this light - also serves other purposes beyond the mere domain registration for customers, in particular also with regard to the functionality of the technical infrastructure as such. Registrar and registry therefore also have to a certain extent a regulatory function, which for example may include participation in the prosecution of legal infringements committed under usage of this ecosystem. Against this background we would consider processing of data for the purpose of maintaining security measures or technical analysis (also operated by third party providers) as likely (depending on the individual case) being justified under Art. 6 (1) lit. f) GDPR.

[26] cf. *Voigt/Pieper*: Impact of the GDPR regarding WHOIS systems", p. 11 et seq.
[27] cf. e.g. in German law Sec. 5 of the Crisis Directive of the German Federal Office of Security in Information Technology, BSI-KritisV, implementing Directive 2008/114/EC

b) Balancing of Interests

However, third party interests in data processing must be balanced against the interests of the data subject. The personal rights of the data subject as well as the effects for the data subject arising from this processing of the relevant data is the starting point of the balancing of interest within the scope of Art. 6 (1) lit. f) GDPR, which is contrasted by the interests of the third party in the specific data processing. To put it in a nutshell: The more substantial the interest of the third party, the more likely disclosure can be justified.

However, stating that there is a general interest for a publicly accessible Whois database considering the role registries and registrars are playing for the functioning of the internet (as outlined above), would be a too broad interpretation of the legitimate interest clause. In its interpretation of Article 7 of the current Directive 95/46/EC that also includes a legitimate interest clause, the Article 29 Data Protection Working Party made quite clear that only those interest may be justified that can be formulated in a sufficiently concrete manner, as a lack of concreteness hinders any balancing of interests.

> "***An interest must be sufficiently clearly articulated to allow the balancing test*** *to be carried out against the interests and fundamental rights of the data subject. Moreover, the interest at stake must also be 'pursued by the controller'. This requires a real and present interest, something that corresponds with current activities or benefits that are expected in the very near future.* ***In other words, interests that are too vague or speculative will not be sufficient.***"[28]

Although this opinion was formulated in view of the current Directive, this interpretation is likely to also apply to the interpretation of Article 7 (f) of the GDPR, as there has been no change in the need for a balancing test.

An important indicator for how to balance interests follows from Recital 47 p. 1, 3. According to it, a balancing of interests must also consider whether a data subject at the time of collection of the

[28] Article 29 Data Protection Working Party: WP 2017, p. 24.

personal data and in light of the circumstances under which it was collected can reasonably foresee that a processing for this purpose will possibly take place. This generally limits the possibilities for justification of data processing activities based on Art. 6 (1) lit. f GDPR. Although it will not be possible to clarify the expectations that were tied to data processing in the specific individual case (so that an objectifying consideration of these expectations must take place) it follows from this that processing cannot be justified if it takes place for purposes that were not foreseeable by the registrant upon registration of the domain. Although the existing public Whois is based on the registrant's contractual consent, it can be argued in this context that registrants know about public disclosure (at least of parts of) registrant data and therefore must assume that personal data provided when registering the domain will be made publicly accessible.

The General Data Protection Regulation itself provides further indications as to which interests can, in principle, be deemed to be justified. Art. 21 (1) GDPR expressly states the establishment, exercise, or defense of legal claims as justification for data processing despite an objection of the data subject. In the context of Article 21 (1) GDPR, however, it is referred to data processing in the context of a data controller´s own claims and responsibilities. However, from this standard it can also be inferred that European data protection law considers data processing in the context of legal claims as interests worthy of protection. This legal valuation even applies to the transmission of data to non-European countries, Art. 49 (1) lit. e) GDPR (see below Part C III 1). This must also affect the balancing of interests within the scope of Art. 6 (1) lit. f) GDPR.

c) Necessity of Data Processing

As a general rule, disclosure of registrant data to 3 [d] parties can only be justified to the extent that it is necessary for the fulfillment of the respective legitimate interest. This principle of "necessity" limits the extent of data disclosure to the minimal means with which the purpose of data processing can be reached. Any data processing exceeding this extent cannot be justified under Art. 6 (1) lit. f) GDPR. For this reason alone, a restriction of the disclosure of the WHOIS data to the data contained in DRL1 is necessary. Further limitations may be necessary depending on the individual interest in data processing.[29] However, the data provided in this set of data is at the same time required as a bare minimum to ensure the fulfilled of the legitimate interests.[30]

[29] For many third party interests, identification of registrants will be sufficient. Therefore it can be argued that email addresses would have to be removed from the data being disclosed, cf. Voigt/Pieper, Impact of the GDPR regarding WHOIS system, p. 3 et seqq.
[30] For details on DLR 1 Part B II. above.

d) Right to Object, Art. 21 GDPR

Under Art. 21 GDPR, every data subject is entitled to object at any time against the processing of personal data based on Art. 6 (1) lit. f) GDPR on grounds relating to his or her particular situation. However, the specific legal meaning of "particular situation" remains open. The recitals also do not contain any further indications. However, it must be assumed that only atypical constellations fall under this clause. For data controllers however, the regulation means that it must take measures to ensure a response to the objection of a data subject in the individual case and that this data is disclosed only if (i) compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or (ii) for the establishment, exercise or defense of legal claims (of the controller). However, the atypical constellations that authorize an objection in the individual case and the compulsory grounds worthy of protection that in the individual case justify the disclosure of data is subject to a case-to-case review.

e) Legitimate 3 d Party Interests for Disclosure of Whois Data

Against the background of the legal standards outlined above, it can be assumed that the balancing of interests will typically justify disclosure of Whois data in the following contexts:[3]

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	DRL 1

[3] Cf. in this regard also *Voigt/Pieper*: Impact of the GDPR regarding WHOIS systems", p. 16; *Nygren/Stenbeck*, gTLD Registration Directory Services and the GDPR - Part 1, p.13; ; Nygren/Stenbeck, gTLD Registration Directory Services and the GDPR - Part 3, p. 8 et seq..

		(or known certification authority) • proof for request for certification by Registrant	

Although we see strong arguments that disclosure can be justified in the above mentioned contexts, this does not necessarily mean that a controller at the same time is under an obligation to do so (e.g. registrars may choose to take down a website rather than to disclose registrant data).

Finally, we should note that the limitations imposed by 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.

4. Other requests

With regard to third party requests, the justifications for disclosure of data outlined above are exhaustive. Any other third party requests, such as general inquiries to the registrant cannot justify disclosure of registrant data. It is therefore advisable that registrars offer either an anonymized email address for the registrants via a web interface or a web form where messages for the registrants can be entered and will then be forwarded to the registrant's email address to ensure anonymity.

5. Note: Data Subject´s Rights, Art. 12 et seq. GDPR

GDPR also contains a number of so called data subject´s rights. In particular, it must be ensured that the person, whose personal is being processed (i.e. in particular the registrant) receives information about his personal data processed by the data controller on request, Art. 15 GDPR. Further data subject rights refer e.g. to the deletion (Art. 17 GDPR) or rectification (Art. 16 GDPR) of data. Consequently registries and registrars must ensure corresponding procedures. The most convenient way to provide those functions within protected customer areas.

6. Disclaimer

The legal requirements for disclosure of Whois data described above exclusively refer to the provisions of the GDPR. Please note that there might be additional limitations of what data can be disclosed under national laws a contracted party might be subject to. The other way around, laws of non-EU member states may entail legal obligations for disclosure of data (e.g. for criminal law enforcement). The resulting conflicts between the different legal systems are not part of the legal assessment in this paper.

III. International Transfer of Data

As noted above, further legal requirements apply to disclosure of (Whois-) data in case data is being transferred outside the EEA. As the current data protection directive, the GDPR stipulates a set of rules for international data transfers to ensure an adequate level of data protection, even if data is being transferred abroad. These requirements (Articles 44 et. seq. GDPR) apply in addition to the general rules on the lawfulness of data processing as such (esp. Article 6 GDPR, see Part C II above). This means in practice, once processing of data (in this case: disclosure) can be justified under Art. 6 GDPR, this does not necessarily mean that transfer of Whois data to non-EU Member States can be justified, too. Similar requirements to those of GDPR exist for the data transfer from European law enforcement authorities to those of third countries on the basis of the Directive (EU) 2016/680.

1. International Data Transfer under GDPR

The GDPR provides various possibilities to justify transfer of data outside the EU, such as

- Article 45 GDPR: Data transfer on the basis of an ***adequacy decision*** by the EU Commission (non-EU states can apply for the EU Commission to issue an adequacy decision that recognises the level of data protection as comparable to EU standards).
- Article 46 GDPR: "***appropriate safeguards***", such as legally binding and enforceable instruments between public authorities or bodies, ***binding corporate rules*** ("**BCRs**") within a group of companies, ***Standard Contract Clauses*** ("**SCCs**") provided by the EU Commission or ***safe harbour*** certification.

More importantly, the GDPR provides further exceptions for international data transfers in certain contexts, Art. 49 GDPR. Data transfer can be justified without the need for an adequacy assessment or appropriate safeguards, among other things, if the transfer is necessary for the performance of a contract between the data subject and the controller (Art. 49 (1) lit. b GDPR), for important reasons of public interest (Art. 49 (1) lit. d GDPR) or if it is necessary for establishing, exercising or defending legal claims (Art. 49 (1) lit. e GDPR):

Article 49 (1) lit. b) GDPR reflects the concept, already laid down for justification of data processing under Art. 6 (1) lit. b) GDPR. According to this provision data processing is justified where it is necessary for the performance of a contract (see above Part C II 1). Article 49 (1) lit. b) GDPR extends this legal valuation to international data transfers. Consequently, where data transfer is necessary for the

performance of the ***dispute resolution programs "UDPR" and "URS"***, a transfer to the non-EU country may be considered as being justified.

Article 49 (1) lit. d) GDPR justifies international data transfer if it is necessary for important reasons of public interest. Article 49 (4) GDPR further clarifies that any third country interest presented in order to justify data transfer under Article 49 (1) lit. d) GDPR must also be recognised either in EU law or in the laws of the respective EU Member State. The scope of this provision is quite limited as only particularly important public interests can be taken into account. In this respect recital 112 explicitly names international data exchange between competition authorities, between tax or customs administrations, between financial supervisory authorities and between services competent for social security matter or for public health. Furthermore, an excessive use of this justification clause for transfers to foreign public authorities may undermine legislative decisions for or against international cooperation with third countries. International data transfer for public law enforcement purposes is regulated within Directive (EU) 2016/680 and is therefore outside the scope of the GDPR.

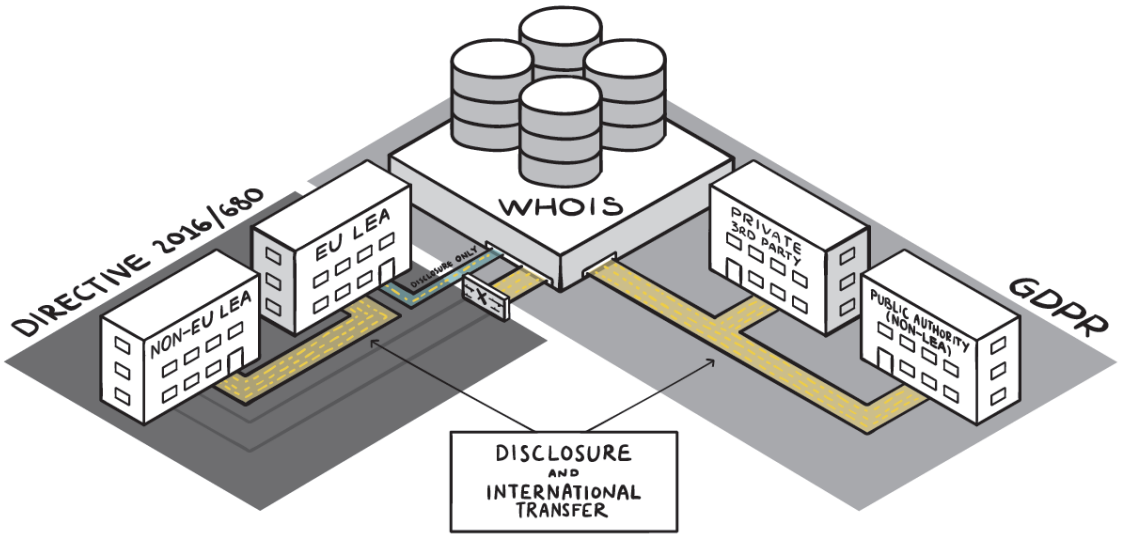
Article 49 (1) lit. d) GDPR further allows international data transfers to non-EU states if it is necessary for the establishment, exercise or defence of legal claims. This provision enables controllers of Whois data to satisfy information demands related to private (IP-) law enforcement from outside the EU. The wording of the provision is not limited to a data transfer in the context of court proceedings. Therefore, the provision also permits data transfer to private parties or public authorities, as long as this a transfer serves the purpose of establishing, exercising or defending of a legal claim (e.g. in administrative proceedings).

The exception for a transfer of personal data accessible within public registers (Art. 49 (1) lit. g) GDPR), however, does not apply to a public Whois directory. This provision only covers registers that are intended to provide information to the public under the laws of the EU or the Member States, such as commercial or land registers. This is not the case with private directories like the existing public Whois.

2. International Transfer of Whois Data to Non-EU Law Enforcement Agencies

According to Directive (EU) 2016/680, European Member States should ensure that a transfer by European law enforcement agencies to a third country or to an international organisation takes place only if necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and that the controller in the third country or international organisation is a competent authority as well. Similar to the requirements for international data transfer according to the GDPR,

such transfers may take place for instance in cases where the European Commission has decided that the third country or international organisation in question ensures an adequate level of protection or, in the absence of an adequacy decision and of appropriate safeguards, certain derogations for specific situations apply (e.g. in order to protect the vital interests of the data subject or another person or for the prevention of an immediate and serious threat to public security of a Member State or a third country).



IV. Procedural Aspects

a) Certification of Public Authorities

All in all, even if the criteria listed above (Part C II 2) are used as a basis for the disclosure decision, there may still be a large variety of legal bases and, therefore, of public authorities acting on the basis of such. In practice, this would lead to the result that, in case of information disclosure requests submitted to registrars or registries, the assessment of the legal basis to be performed might be extremely complex and difficult and require significant administrative efforts and time, for which quite a number of resources would have to be provided. Said effort and time increases with the number of expected requests. In 2014, for example, Deutsche Telekom, alone, disclosed the owners of 733,377

IP addresses, which in accordance with European law must also be considered personal data, to law enforcement authorities[32].

In addition, in case of the investigation and prosecution of criminal offences it has to be generally assumed that the request of the public authority is urgent. An individual assessment of all requests for information would stand in opposition to the urgent need for information of the public authorities; even misjudgments of the assessor could not be excluded.

A registration and/or certification of public authorities lend itself as a possible solution for preventing this. Thus, a case-by-case assessment based on the criteria shown above would not be necessary and quick access for the public authorities would be ensured.

In this context, in a registration and/or certification process, first of all an assessment based on formal criteria can be conducted in order to assess whether or not the respective public authority may be entitled due to a legal basis to request information on the ownership of a domain (at the same time constitutes justification for data disclosure under Art. 6 (1) lit. c) GDPR for the registry/registrar).

After the certification, the public authorities would be able to view the DRL 1 data of such domains which are relevant e.g. in connection with the investigation of a criminal offense.

In a policy for the use of the data, any public authority would furthermore be obligated

- not to perform abusive or mass data inquiries,
- not to forward the obtained data to unauthorized third parties.

Once certification took place on this basis, access to DRL 1 data can be given within the scope of terms of use.

Although disclosure of data would not be strictly limited to individual registrant data, the effects to the registrant arising from a certification model compared to a generally publicly accessible WHOIS directory significantly lowers the impact on the data subject due to strict access restrictions and

[32] Cf. https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/archiv-datenschutznews/news/transparency-report-2014---cooperation-with-government-agencies-362418.

purpose limitations. The impact to the registrant´s right and freedoms can be further reduced by implementing technical measures like

- limitation to inquiries for individual domains
- limitations of the total numbers of queries
- localization of the request based on IP address
- the use of CAPTCHAs

However, there are also critical voices about such a model. Their argument is that access by "automatically qualified parties" that have been qualified within a certification process cannot replace the required legal assessment in each individual case.[33] This argument cannot be completely dismissed. However, even if direct access based on certified access only should not be legally possible, certification of those authorities being entitled to request information at all would already be a considerable facilitation of the process justifying the effort.

b) Certification of Private 3rd Parties

Such certification model could also be used for information requests from private 3 d parties. The certification process would need to fulfill at a minimum the following criteria to justify disclosure of registrant data:

Firstly, the certification would from the start be restricted to the limited group of 3 d parties typically having legitimate interests in disclosure of Whois data (as outlined above).

For the registration itself, the applicant would need to provide evidence concerning the association with one of those 3 d party groups. This may take place e.g. through electronic transfer of an attorney's ID card or the excerpt of the register of the association or the chamber of commerce, as well as providing details like organization's websites etc. The precise modalities of registration can also be oriented toward the respective national specifications (e.g. reviewing the listing in a publicly accessible attorney's directory, if available).

Further, the request would have to be filed by a person authorized to represent the respective 3 d party group. In a policy for the use of the data, any applicant would furthermore be obligated

- not to perform abusive or mass data inquiries,

[33] Cf. Nygren/Stenbeck, gTLD Registration Directory Services and the GDPR - Part 3, p. 11.

- not to perform data inquiries for advertisement or direct marketing purposes;
- only to view data if this is necessary to establish, exercise or defend legal claims,
- not to forward the obtained data to unauthorized third parties.

Once certification took place on this basis, access to DRL 1 data can be given within the scope of terms of use.

Although disclosure of data would not be strictly limited to individual registrant data, the effects to the registrant arising from a certification model compared to a generally publicly accessible WHOIS directory significantly lowers the impact on the data subject due to strict access restrictions and purpose limitations. The impact to the registrant´s right and freedoms can be further reduced by implementing technical measures like

- limitation to inquiries for individual domains
- limitations of the total numbers of queries
- localization of the request based on IP address
- the use of CAPTCHAs

Note:

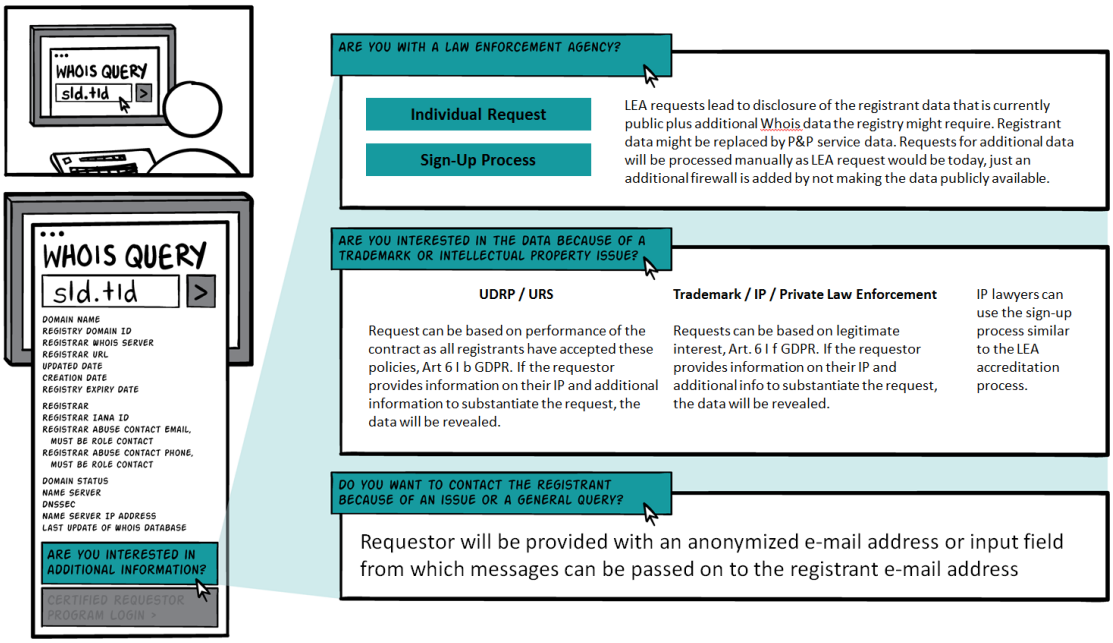
RDAP makes it possible for CAs to issue certificates granting tiered access based on pre-defined parameters. Certification can therefore be granted for multiple contracted parties and must not be conducted with each and every contracted party.

c) Logical Structure of a Disclosure Process

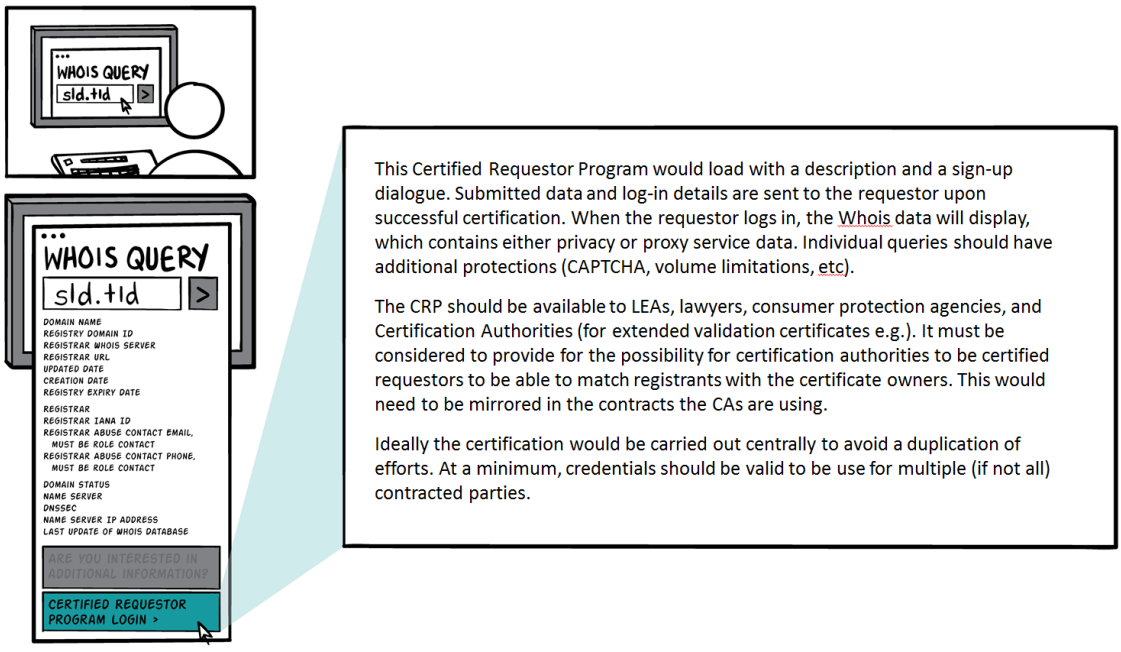
If a requestor types in a Whois query on a domain name, the Whois query will return data that comes from the registrar, including

- 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.

In case 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 GDPR, requestor will be provided with an anonymized email address or a web form from which messages can be sent to the registrant email address.

V. Proposal of a Trusted Data Clearinghouse (TDC)

A GDPR compliant WHOIS system mandatorily results in the fact that a more efficient process must be found, which at the same time continues to provide access to the authorities and 3 [d] parties outlined above.

The outlined procedure for processing information requests will entail an extreme organizational and procedural effort both for the requesting party as well as for the responsible entity, because the inquiring party would first have to research the competent registrar or registry for the respective domain to which it must address its request for information. The relevant contact partners and its contact information must then be discovered, in particular in urgent cases.

An expertly qualified and trustworthy instance as a neutral information broker could coordinate access to the relevant WHOIS data and handle the parties' relevant obligations to data disclosure to unify this process on a global level for all players participating in it. This Trusted Data Clearinghouse (hereinafter "TDC") would operate a platform on which the outlined registration certification process would be set up for the identified group of authorities and 3 [d] party groups authorized to receive information.

Only data category DRL 1 would be accessible through this platform. This category includes in particular name and contact details of the registrant as well as the time of domain registration and thus provide authorized entities with the information concerning the entity that is legally responsible for registration of the domain. Based on this, interests concerning public law enforcement as well as the legitimate interest in the establishment, exercise or defense of legal claims under civil law (e.g. to prosecute copyright or trademark violations) would be possible.

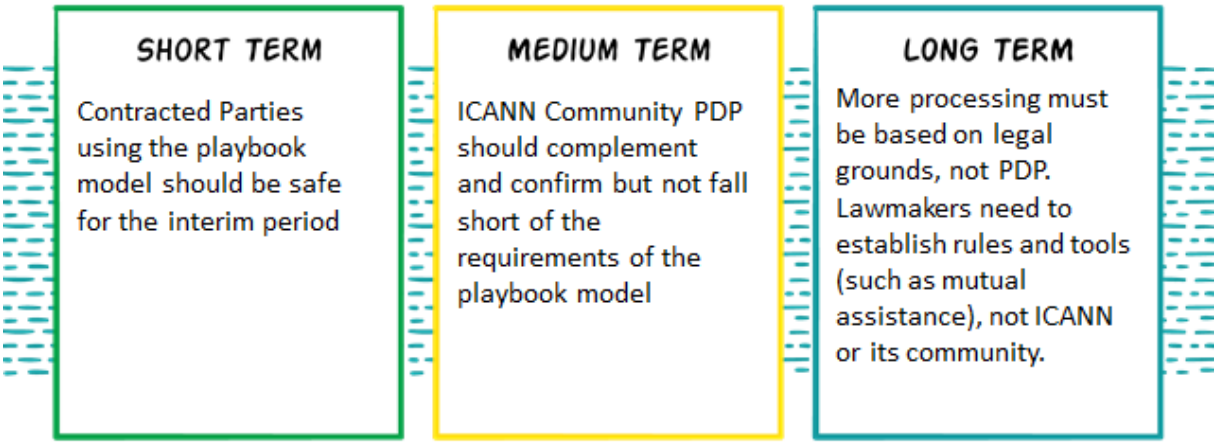
Further, a communication tool could be set up for non-certified requestors through which the TDC mediates contact to the domain owner and leaves it up to the domain owner to either contact the inquiring party or to consent to the disclosure of its data.

With regard to information for the prosecution of claims under civil law, this system would be restricted only in cases in which the registrant asserts its right to object under Art. 21 GDPR. As presented above, European registrants are entitled to object to the processing of their personal data for grounds relating to their "particular situation".

The TDC could also handle the processing of these objections. The registrars and registries would provide a corresponding email address within the scope of their obligation to refer to the existence of this right to object in their privacy notice. Any objections received at would then be legally analyzed by the TDC to review whether a right to object exists in the individual case. If that is the case, data can be anonymized, or at least disclosure of such data to requestors can be denied. Art. 21 (1) GDPR generally provides that the interests of the responsible entity in data processing can in particular be predominant if the processing serves the assertion of legal claims, but the regulation here means legal claims in the relationship between the responsible entity and the data subject, not legal claims of third parties decisive here, e.g. of originators or trademark owners.

Part D – Outlook

Ideally, the contracted parties would agree on a joint data model with ICANN.
Implementation of the playbook model in a timely fashion poses an additional challenge to all parties involved. Technical implementation needs to be done, 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.


SHORT TERM
Contracted Parties using the playbook model should be safe for the interim period
MEDIUM TERM
ICANN Community PDP should complement and confirm but not fall short of the requirements of the playbook model
LONG TERM
More processing must be based on legal grounds, not PDP. Lawmakers need to establish rules and tools (such as mutual assistance), not ICANN or its community.