GDPR
Domain Industry Playbook

v.06

PLEASE NOTE A SUMMARY IS PROVIDED WITH A SEPARATE DOCUMENT

Authors:

Julia Garbaciok*
Andreas Konrad**
Martin Lose*
Thomas Rickert**
Jan Schlepper**
Oliver Süme*

*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 that not only contracts need to be reviewed, but also 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 shall not be construed as legal advice. All parties involved need to work on their GDPR compliance individually, which goes far beyond the topics discussed here.

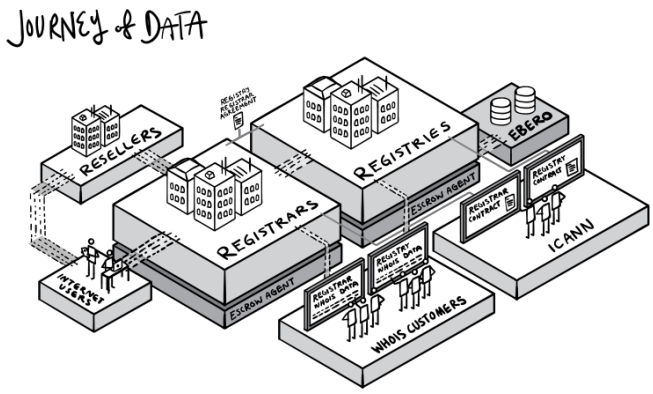
This paper only deals with the data elements ICANN currently requires the contracted parties to process.

Also, 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. Using a Registry Service Provider or a “Registrar as a service” model requires particular attention.

Data flows will be analyzed encompassing the parties typically involved in a domain name registration and as required by ICANN organization in its contracts. The below visualization 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 paper.

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



Note this illustration does not include outsourcing such as RSPs or Registrar-as-a-service models as well as 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 to allow for a holistic view at the data flows and offer a basis for implementation.

While the currently used data records are mentioned 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 bearing 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 develop 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 level.

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 that.

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 might be applicable. The legal assessments[1] available have provided more details on this, so we will not repeat the reasoning here, but 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 be circular reasoning. It has to be reviewed 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 them.

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

[1] Hamilton: https://www.icann.org/en/system/files/files/gdpr-memorandum-part1-16oct17-en.pdf; Taylor Wessing: 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

There are risks associated with proof, 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 sum,

- 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.

Absent 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 speaks to all personal data and such approach should not cause issues with ICANN Contractual Compliance.

- ICANN will support the approach taken for this paper not to limit the legal assessment of data processing to only one legal basis, but instead support a model to allow 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 a minimum set of data that is necessary for registrars to complete the domain name registration process ("Registrar Minimum Data record"). That data falls into DRL1.

Please note these data records may vary bases on the requirements particularly of the registries. Some registries have nexus or other eligibility requirements, while others don't, to give just one example. However, such data would still fall into DRL1 as it is required to perform the contract.

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

As a second step, we will analyze what processing can be based on a legitimate interest. This is particularly relevant to the question of disclosing / publishing data via Whois or otherwise.

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

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

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

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 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 solution imaginable.

The solution offered will be offered for comment and consultation. It could be used on an as-is basis for the interim phase until such time when 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. Using e.g. 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 make 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 as well 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 illustrates the data required by the various participants (see illustration below) within the scope of registration 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. Below we accordingly show the relevant data in this respect.[2]

Note that no differentiation is made here as to 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

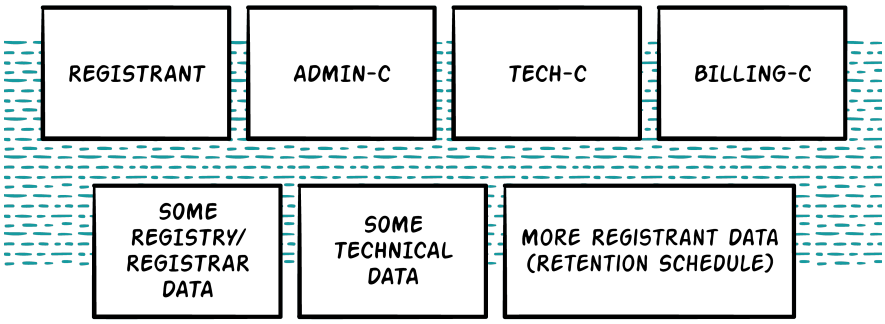
[2] https://www.icann.org/en/system/files/files/draft-gdpr-dataflow-template-registration-data-elements-29jun17-en.pdf

Domain Status
Registry Registrant ID
Registrant Fields • Name • Organization (opt.) • Street • City • State/province • Postal code • Country • Phone • Phone ext (opt.) • Fax (opt.) • Fax ext (opt.) • Email
2nd E-Mail 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 Drivers 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
Transfer Contact Drivers License
Transfer Contact Passport
Transfer Contact Military ID
Transfer Contact State/Government Issued ID
Transfer Contact Birth Certificate
Those objects necessary in order to offer all of the approved Registry Services

To facilitate understanding, the above data elements can be categorized as shown in the following illustration.



It is our recommendation not to abandon the thick registry data model. Also, we will not recommend any changes to be made to the individual data elements / fields. However, the below analysis will show, which of the data elements mentioned above can legitimately collected and how they can be processed. Where data elements cannot be processed, the respective data fields will be populated with syntactically correct place holder data for technical reasons.

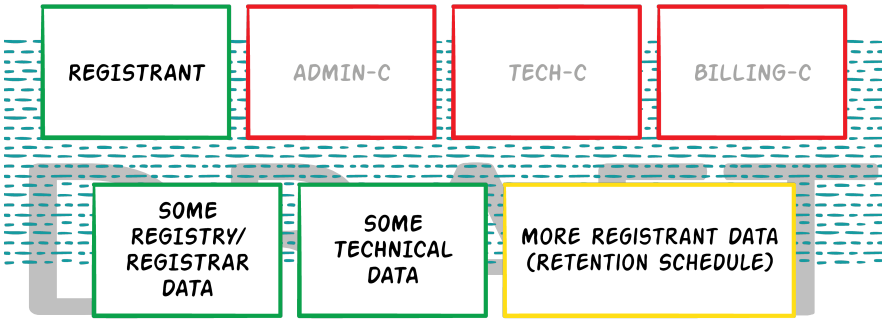
2. ICANN requirements

According to the data model proposed with this document, ICANN shall and can specify the data to be collected with obligatory effect for the participants, because even if 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 that 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 must mandatorily 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. It is here 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 whose 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 "necessary":

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

Kommentiert [A1]: Heading was updated

Kommentiert [A2]: Heading was removed

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

However, input from DPAs should be sought whether a distinction could be made based on a self-identification by the registrant. Should that be an acceptable safeguard, different treatment could be considered.

bb) Technical Data

The registrar collects the following technical data from the registrant to pass such 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

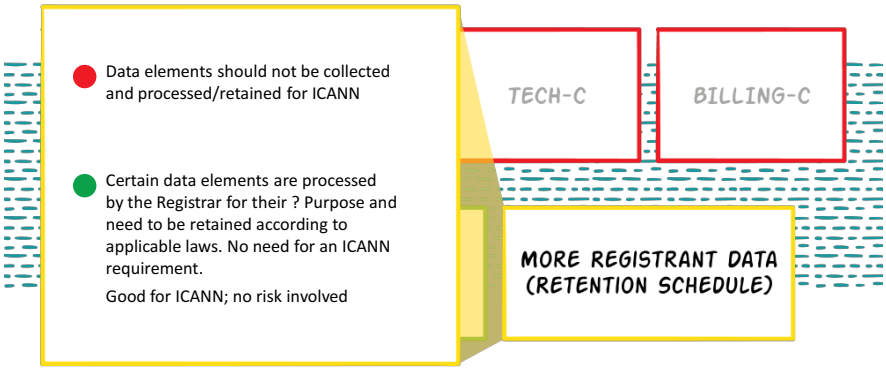
A specification by ICANN on the collection and processing of this data is not appropriate because this data is not necessary for maintenance and stability of the DNS. Only the registrar requires the stated data for its performance of the contract vis-a-vis a contractual partner. In this respect, a compulsory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

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

Basic Setup: Data Risk Level 1 > Registrar



The data in the data retention schedule might 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 s 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 still is relevant under data protection law. The registrar's own employee data disclosed here by the registrar itself for contacting is necessary for fulfillment of the contract to offer the registrant 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 to manage and process its internal contract handling. In this respect it is necessary that the registrar can allocate the domains registered through its service to specific customers to allocate and implement inquiries and requests within the scope of domain management pursuant 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 here also necessary in case of problems or other anomalies with regard to the domain name.[3]

The current procedure for domain name transfers via email communication cannot be continued due to GDPR requirements. At present, e-mails can be sent to the Admin-C to get transfers confirmed. Absent Admin-C data being collected, the transfer process needs to be revised. Additionally, as can be seen in Part C of this document, the registrant's e-mail address will not be published anymore.
Therefore, we suggest to establish a new system based on secure auth-codes with the possibility to revoke transfers within a reasonable timeframe. For 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. Alternatively, transfers can still be carried out without having an e-mail address published by means of communication between the registrars. Since the Inter Registrar Transfer Policy allows for

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

contacting either the registrant or the admin-c e-mail address, it would need to be clarified that only the registrant e-mail address must be used for transfers.

We should note that registrars in discussions about new ways to facilitate transfers at present that could contribute to a solution.

cc) Abuse

This may also include cases in which the domain is abused externally by third parties as well as cases in which it is suspected that the registrant itself performs an infringing act. The registrar must further also be able to fulfill legitimate claims of third parties with regard to the domain or the relevant registrant. In this respect, there is frequently a need to quickly establish contact the customer.

dd) Ownership position

The registrar has an interest to quickly and directly contact 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.

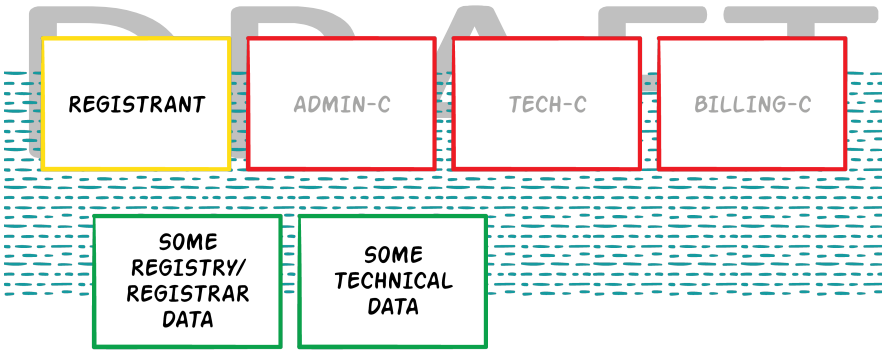
In this case, data collection may be justified even if a registration can ultimately not be executed because the justification pursuant to Art. 6 I b) GDPR also captures precontractual measures. Furthermore, the registrar's effort to register represents the content of the order vis-à-vis the

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 particularly 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

Kommentiert [A3]: Heading was changed

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

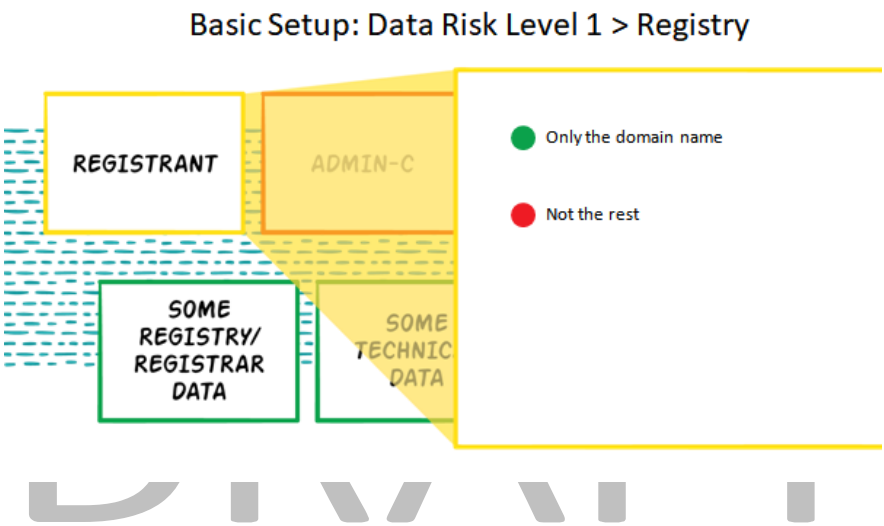
From data protection aspects, only the domain name is relevant for the registry as potentially personal data.

However, there has been a policy development process including all ICANN stakeholders confirming by way of a consensus policy that is binding for all contracted parties, that a thick Whois model should be maintained by all registries. Reasons have been archival and restoration purposes as well as improving the data quality. We are seeking input from the DPAs whether such policy can be used as a justification for the transfer of registrant data from the registrar to the registry and for such requirement to be enforceable by ICANN. That does not mean that such data shall 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, so that this data currently is 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 as to whether the relevant domain represents personal data or not causes major problems in practice, therefore we are considering all domain names to be personal data within the scope of this opinion.

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 directly possible by the registry itself has no effect on the qualification as personal data.

In this respect, the European Court of Justice (ECJ) concerning a similar case situation[4] – the storage of dynamic IP addresses of visitors at websites of official authorities - has 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 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. This disclosure in the present model is specifically possible only by the registrar.

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 be open also with regard to legal persons, if and insofar as the enterprise name of a legal person itself may contain name components enabling an allocation to a natural person.

bb) Result

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

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

b) Reasons

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

The listed data is 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.

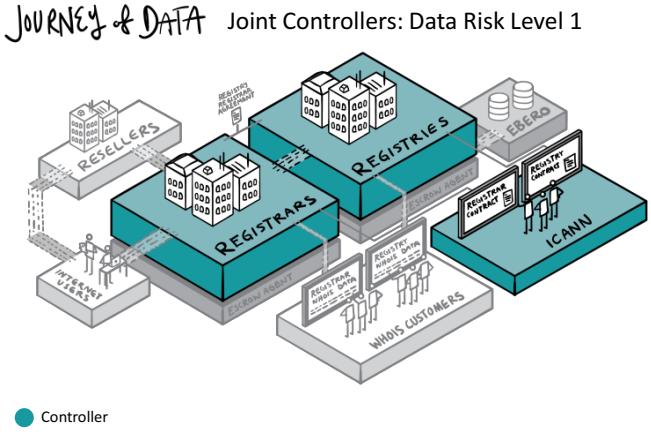
3. Data controller

Within the scope of the suggested data model, the question arises as to who the responsible entity is for processing DRL 1 registration data, in particular because only very few 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.

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 commissioned by ICANN states that due to the complexity of processing structures it is recommended to assume joint responsibility between ICANN, registrar, and registry (Memoradum gTLD Registration Directory Service and the GDPR, Part 1, Section 3.7.3), also because this 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 the manner that 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) Differentiation of processor vs. 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.[5]

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"[6].

Processors must be differentiated 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.
- Processors are independent legal persons that are different from the controller and which process data on behalf of the controller(s) without deciding on the purposes of processing.[7]

(ii) Purpose of Art. 26 GDPR

The regulation is to primarily serve the protection of the rights and freedoms of data subjects.[8] 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.[9]

"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

[5] *Klabunde* in *Ehmann/Selmayr* „Datenschutz-Grundverordnung" Art.4 marg. no. 29
[6] 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
[7] 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
[8] *Bertmann* in *Ehmann/Selmayr* „Datenschutz-Grundverordnung" Art. 26, marg. no. 1
[9] 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

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."[10]

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.

Only the registrar appears vis-à-vis the registrant as it coordinates the complete handling of the registration and maintenance of it. 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.

(iii) Set of operations

Further, 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 operations "domain registration" 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 scope of the processing chain of smaller processing steps in detail 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 applies here specifically (Art.29 Group WP 169, p. 25).

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 must be differentiated here. This data fulfils another purpose that is not codetermined by the registry.

[10] 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

(iv) 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 is responsible

*"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; and"*

As already stated, ICANN fulfils this responsibility among other things by contractually specifying vis-à-vis 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.

(v) 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 pursuant to 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 several 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 several 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, it is to 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,

- against 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 to the registrant.

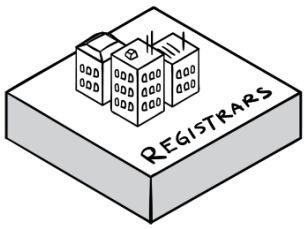
(6) Procedure record

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

cc) Responsibility for other data

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

Can the Registrar add data elements?



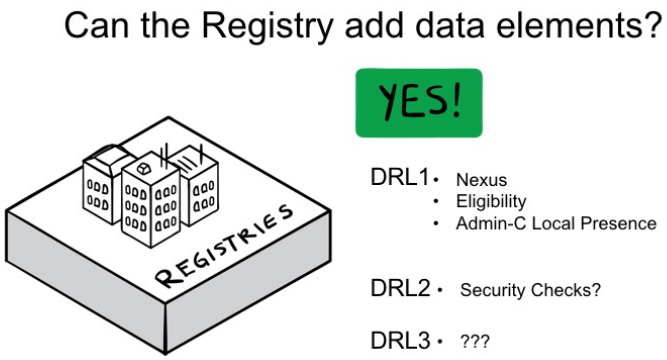
YES!

- No involvement of Registry, ICANN, or Escrow Agents
- At their own risk

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 can be added by the registry, which are not belonging to DRL1. However, all registry requirements going beyond the minimum data set need to be explicitly spelled out in the RRA. Where no such requirement is 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 serves 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 located with regard to eligibility requirements under 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 to find information from admitted 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 consists specifically in maintaining the exclusivity of these relevant online spaces and to offer 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 to the verification. Due to the multitude of TLDs and their requirements it is not possible to illustrate all TLDs and their additional requirements to registration authorization in each individual case here, thus 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 in any case is performed on behalf 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 processor of the registry for this additional data as well. The registrar does not have 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. Outsourcing the review of the registration authorization to the registrar in a manner that the registrar independently determines the means and purposes of the collection of the additional requirements for the registration authorization as well as an independent review of the additional requirements at its own responsibility under data protection law is not feasible, because in this respect it is incumbent upon the relevant registry to itself ensure the existence of the requirements placed by itself to 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 security, stability, and resiliency of the DNS. To meet this responsibility, ICANN among other things imposed the stated obligations through the registry/registrar data escrow program. This is 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 and worthy of protection for economic reasons.
The same applies to the registry data available at the registry.

4. Affected data

To fulfil 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 necessary quantity. In this respect, logically, the transmission of all this data is also compulsory to achieve the purpose of safeguarding in the event of a loss. This applies equivalently 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 and the retained data from the escrow agent must be transmitted to ICANN or another registrar.

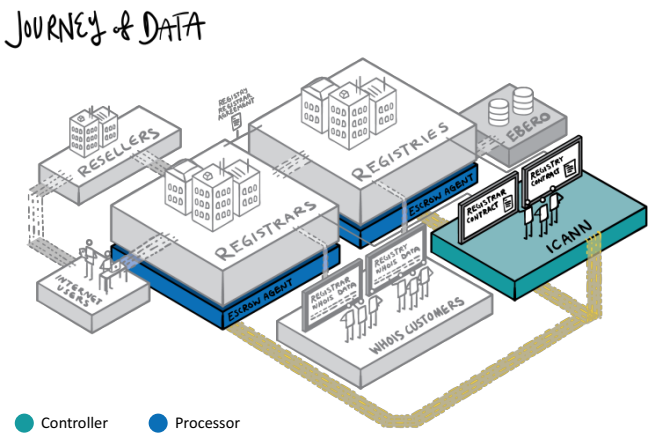
5. Responsibility

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.

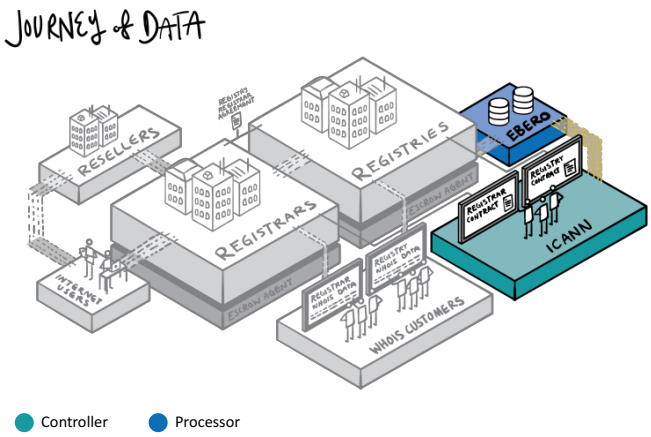
As soon as and insofar as any emergency event occurs that affects data of data subjects that is retained at the escrow service and falls under the GDPR, a GDPR-conform EBERO is necessary.

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 necessary quantity. Insofar, the transfer of all this data is logically also compulsory to maintain the purpose of safeguarding 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

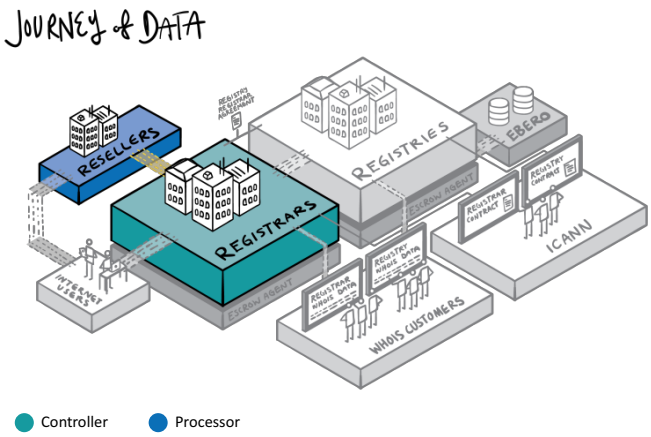
Insofar as the domain registration order is received by the registrar through a reseller (or a multitude of resellers), various data processing operations with various responsibilities exist.

1. Responsibility

The reseller collects the same data at the registrant that the registrar would also collect directly [11] and thus in part takes the place of the registrar. However, the reseller shall 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.

[11] See above Part B II. 1.



a) Account Data

In this regard, the contractual partner's account data is collected by the reseller at 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 exclusively the data necessary for registration. The relevant registry and the registrar determine this data and therefore they chiefly decide on the purposes of data processing.

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 best interest 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, which can be performed only by the registrar, to it. 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 therefore are subcontractors of the respective reseller, because all parties in the chain are active merely 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, in deviation 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 might be other data that the registry might 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.

1. Authorization

The data listed here is not data that has obligatory necessity for contract fulfillment under the model suggested here. 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 dominate within the scope of a 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. In this respect it may specifically be necessary that the registry for this purpose receives 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.

b) Central management

The central management in term of an equivalent to a commercial register, land register, or birth register as well as the patent and trademark register may also be seen 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.
The registry as responsible entity for the namespace operated by it can also assert a legitimate interest in the ability of allocating and identifying the relevant registrants for which it provides services under the responsibility 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 principal standardized in Art. 5 (1) lit. c) GDPR because in this respect the registry is also justified to retain 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.

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.

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.[12]

[12] 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.

1. Legally Ineffective Consent

Section 3.7.7.5, the RAA 2013 requires that the registrant must consent to the data processing. 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.

2. No Justification under Statutory Law

Likewise, none of the statutory circumstances 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

organization of internet communications and, therefore, also of domain registration has always been performed on the basis of private legal relationships. This is why a public regulatory framework, which would e.g. also require for 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 data subject on the other hand on a case-by-case basis. It is true that there is a variety of reasons why certain authorities, individuals or groups of individuals have profound interest in accessing Whois data and therefore leading to a justification of disclosure (e.g. for identification of a person who has registered a certain domain) under GDPR.[13] 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 and towards persons other than the holder of a legitimate interest.

For these reasons, a closed WHOIS system which can be accessed in individual cases only (namely if a justification under data protection law exists) and/or from which information is provided in individual cases will be required once GDPR enters into effect. Compliance with the provisions of the regulation is particularly important for any provider of a Whois database, as violations can result in significant fines.

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

The EWG final report has established a list of Whois users and their respective interests in accessing Whois data[14]. The gTLD Registration Dataflow Matrix and Information document also lists users and use cases[15], 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. First of all, the criteria for individual requests are to be examined

[13] 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.
[14] ICANN: EWG final report on gTLD Directory Services, p. 21.
[15] ICANN: Draft dTLD Registration Dataflow Matrix and Information.

(1.). In a second step, a procedure for handling information requests in practice is to be proposed (2.). Finally, we provide a proposal for a Trusted Data Clearing House for the domain industry (3.).

1. Legal Grounds and Criteria for Disclosure

There are different groups of 3rd 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. 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.

a) 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. To the extent necessary for these programs, data processing including disclosure of personal data is therefore admissible. 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.[16]

[16] 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.

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

It is 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 corresponding legal basis in the laws of the EU or the Member States.[17] 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 justification of disclosure requests of public authorities of non-EU states on the basis of Art. 6 (1) c) GDPR cannot be justified. 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.

"Legal obligations" in the meaning of Art. 6 (1) lit. c) GDPR do not necessarily require acts of parliament.[18] Therefore, different kinds of substantive law provisions can be considered as legal basis for disclosure (e.g. regulations and statutes on the basis of which public authorities such as law enforcement authorities or financial authorities are given competences or investigation rights). As a general rule, 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, 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*[19]. Finally, Art. 6 (3) GDPR provides a catalogue of specifications with regard to the content

[17] Recitals 40 and 45.

[18] 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.

[19] 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

of the required legal basis. This exemplary list can be consulted 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.

Accordingly, 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.[20]

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:

- 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.
- Legal bases under national law must be specified from which the right to view the 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, in the case of law enforcement authorities, for example, exclusively for purposes of criminal prosecution.

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.

[20] Cf. Recital 41; also consider Recital 45, pursuant to which a law can also be the basis for several processing operations.

c) 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 third country authorities cannot be justified. Recital 47 demonstrates 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 3rd country authorities than to authorities of the EU or EU member states.

aa) "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 coming 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 [21]. Recital 47 p. 2 furthermore mentions customer relations and the service relationship 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

[21] cf. *Voigt/Pieper*: Impact of the GDPR regarding WHOIS systems", p. 11 et seq.

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 .[22] The activity of Registry and Registrar - in this light - also serves other purposes beyond the mere domain registration to customers, in particular also with regard to the functionality of the technical infrastructure as such. Registrar and registry therefore to a certain extent also have a regulatory function, which for example may include participation in the prosecution of violations 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.

bb) Balancing of Interests

However, 3rd 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.

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

[22] 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

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 Whois system 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 must also affect the balancing of interests within the scope of Art. 6 (1) lit. f) GDPR.

cc) Necessity of Data Processing

As a general rule, disclosure of registrant data to 3rd 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. 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.[23]

dd) 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

[23] For details on DLR 1 Part B II. above.

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.

ee) Legitimate 3rd Party Interests for Disclosure of Whois Data

Against the background of the outlined legal standards, it can be assumed that the balancing of interests will typically justify disclosure of Whois data in the following contexts:[24]

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

[24] 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.

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.

d) 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 e-mail 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 e-mail address to ensure anonymity.

e) 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.

f) 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.

2. Procedural Aspects

a) Certification of Public Authorities

All in all, even if the criteria listed above 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[25].

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.

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

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

b) Certification of Private 3rd Parties

Such certification model could also be used for information requests from private 3rd 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 3rd 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 3rd 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 3rd 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,
- 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:

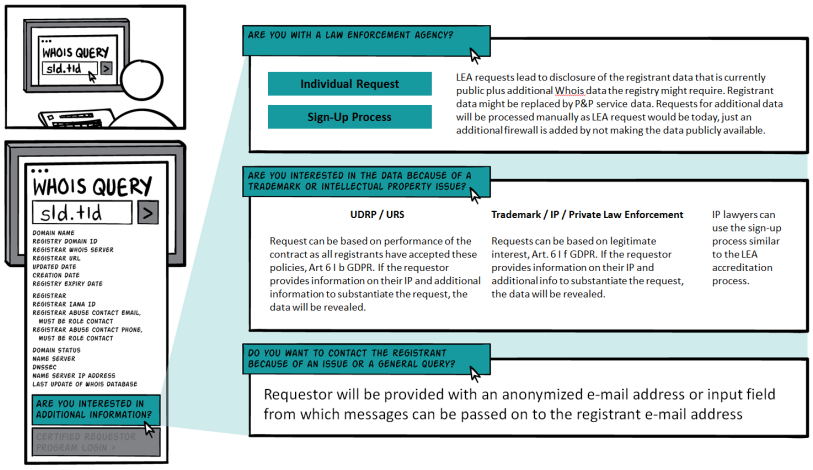
RDAP makes it possible for CAs to issue certificates granting tiered access based on pre-defined parameters. Certification can therefore be granted for multiple contracted parties and must not be conducted with each and every contracted party.

c) Logical Structure of a Disclosure Process

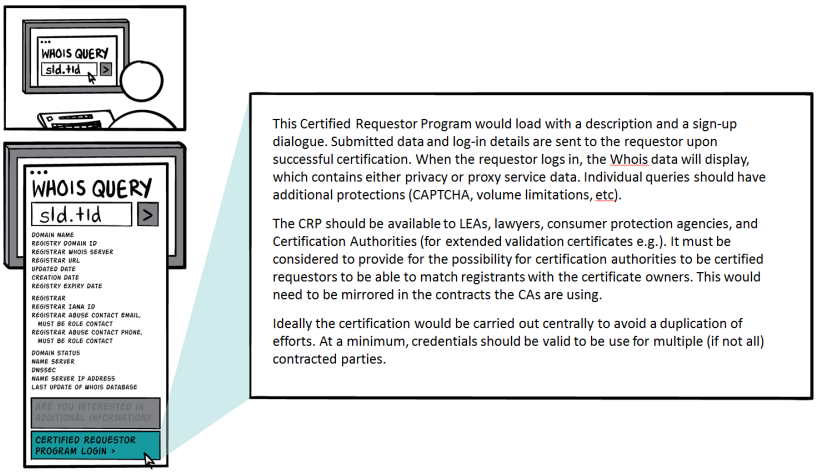
If a requestor types in a Whois query on a domain name, the Whois query will return data that comes from the registrar, including

- 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 e-mail address or a web form from which messages can be sent to the registrant e-mail address.

3. 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 3rd 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 3rd 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.

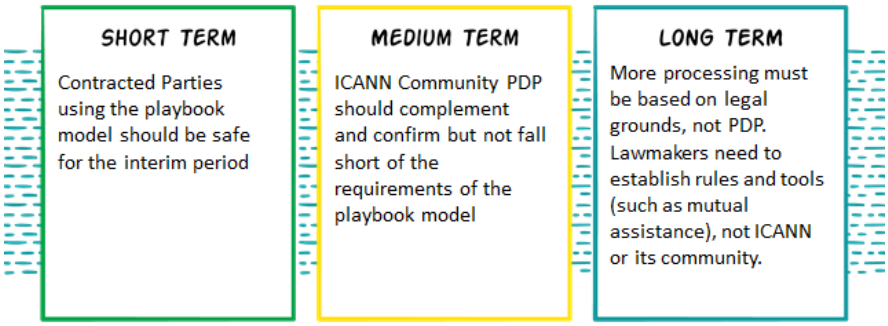
Further, a communication tool could be set up for non-certified requestors through which the TDC mediates contact to the domain owner and leaves it up to the domain owner to either contact the inquiring party or to consent to the disclosure of its data.

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.