GDPR
Domain Industry Playbook

High Level Summary

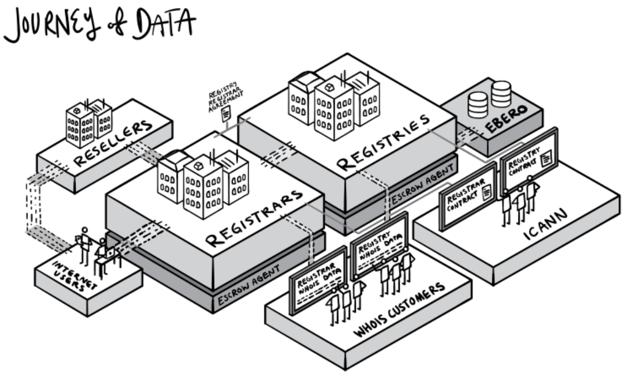
v.06

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

Key findings – Collection and “internal” processing



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

- DRL 1 – Low risk – Performance of a contract (Art. 6 (1) lit. b) GDPR)
- DRL 2 – Medium risk – Legitimate interest (Art. 6 (1) lit. f) GDPR)
  - The data subject has the right to object, but balancing of rights follows
- DRL 3 – High risk – Consent (Art. 6 (1) lit. a) GDPR)
  - The data subject can withdraw consent at any time without any reason

Illustration 1

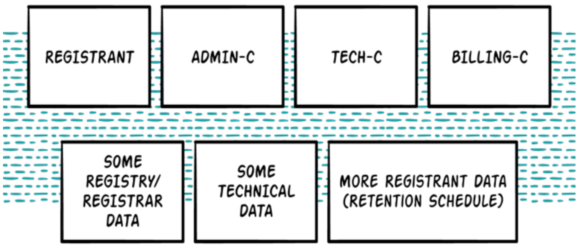
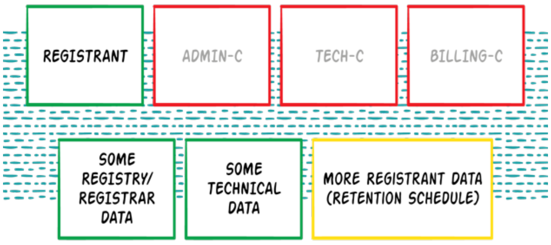

REGISTRANT
ADMIN-C
TECH-C
BILLING-C
SOME REGISTRY/ REGISTRAR DATA
SOME TECHNICAL DATA
MORE REGISTRANT DATA (RETENTION SCHEDULE)

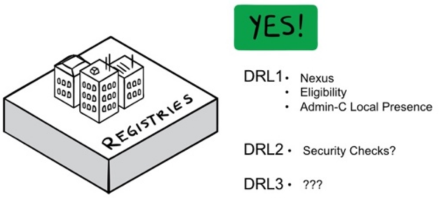
Illustration 2


REGISTRANT
ADMIN-C
TECH-C
BILLING-C
SOME REGISTRY/ REGISTRAR DATA
SOME TECHNICAL DATA
MORE REGISTRANT DATA (RETENTION SCHEDULE)

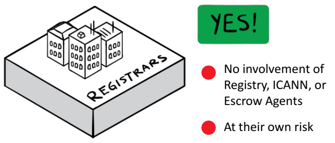
- Illustration 1 shows categories of data that are required to be processed today. Much of that data is not personal. Some of the registry / registrar data can be personal data, but we trust the companies can make sure this is processed in a compliant fashion.
- **Registrants may be natural or legal persons. Therefore, the question arises 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.**

- **Registrars:** Illustration 2 shows the proposed set of data that constitutes registration data in the proposed model. Admin-C, Tech-C and Billing-C will not be needed anymore. Registrant data can be collected by the registrar or their resellers in DRL1. No changes are recommended to be made to the other data elements. However, the data in the yellow box (data retention specification) shall not further be collected based on an ICANN requirement, but according to laws applicable to the registrar or reseller.
- **Registries:** To carry out and maintain the domain name registration, registries do not need the registrant data, but is must be discussed with DPAs whether ICANN policy on Thick Registries can be used as a legal basis for data being stored with the registry. Apart from that, registries can specify additional requirements in the Registry Registrar Agreements according to which they can obtain data in case of nexus / eligibility requirements (DRL1) or based on legitimate interests such as security checks (DRL2).

Can the Registry add data elements?



Can the Registrar add data elements?



- **Responsibilities**
  - For registration data, the registrar, the registry and ICANN are joint controllers.
  - For data escrow, ICANN is the data controller and the escrow agents are data processors.
  - The EBERO is the data processor on behalf of ICANN, the data controller.
  - In reseller situations, the reseller is the data processor on behalf of the registrar for registration data.

Key findings - Disclosure of Data

- Public Whois is not sustainable in its current form.
- In order to allow for the consistent provision of information, information from different sources should be compiled by means of RDAP (delegated Whois). Furthermore, it needs to be clarified that, even at this point, registries and registrars 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 when gated access is provided. Disclosure by privacy or proxy services would be based on the principles applied today and remain unaffected.**
- There are instances in which data can be disclosed. These are
  - Disclosure to fulfill the contract (requests in conjunction with the preparation of URS and UDRP claims), Art. 6 (1) lit. b) GDPR;

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

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

- We should note that the limitations imposed by GDPR will have significant impact on companies and individuals working on safety and security issues. These limitations should be discussed with DPAs with the goal of finding solutions that allow for efficient work on IT and network security.
- The legal basis for disclosure to law enforcement agencies is limited to authorities acting on the ground of EU law or national laws of EU member states.
- It is proposed to establish a certification program for certain user groups (public and private) and give Certified Requestors access to Whois data (which can be privacy or proxy service data)

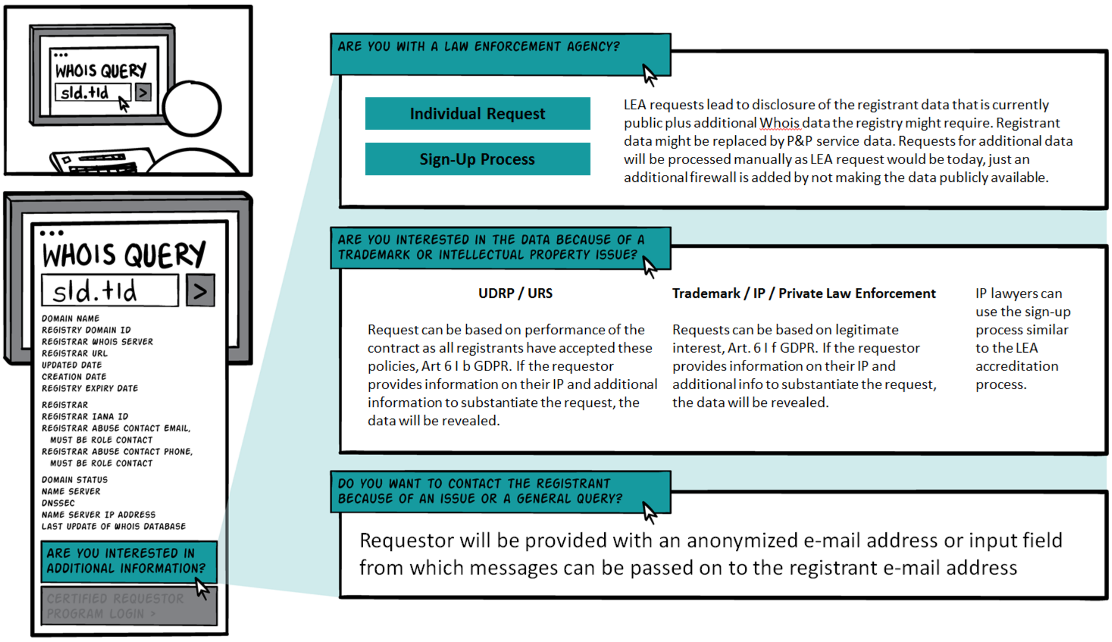
based on pre-defined criteria and limitations (such as captcha, volume limits etc) and only to certain data sets. Limitations could be based e.g. on the country of registrant.

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

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

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

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


WHOIS QUERY
sld.tld
>
WHOIS QUERY
sld.tld
>
DOMAIN NAME
REGISTRY DOMAIN ID
REGISTRAR WHOIS SERVER
REGISTRAR URL
UPDATED DATE
CREATION DATE
REGISTRY EXPIRY DATE
REGISTRAR
REGISTRAR IANA ID
REGISTRAR ABUSE CONTACT EMAIL, MUST BE ROLE CONTACT
REGISTRAR ABUSE CONTACT PHONE, MUST BE ROLE CONTACT
DOMAIN STATUS
NAME SERVER
DNSSEC
NAME SERVER IP ADDRESS
LAST UPDATE OF WHOIS DATABASE
ARE YOU INTERESTED IN ADDITIONAL INFORMATION?
CERTIFIED REQUESTOR PROGRAM LOGIN >
ARE YOU WITH A LAW ENFORCEMENT AGENCY?
Individual Request
Sign-Up Process
ARE YOU INTERESTED IN THE DATA BECAUSE OF A TRADEMARK OR INTELLECTUAL PROPERTY ISSUE?
UDRP / URS
Trademark / IP / Private Law Enforcement
DO YOU WANT TO CONTACT THE REGISTRANT BECAUSE OF AN ISSUE OR A GENERAL QUERY?

LEA requests lead to disclosure of the registrant data that is currently public plus additional Whois data the registry might require. Registrant data might be replaced by P&P service data. Requests for additional data will be processed manually as LEA request would be today, just an additional firewall is added by not making the data publicly available.

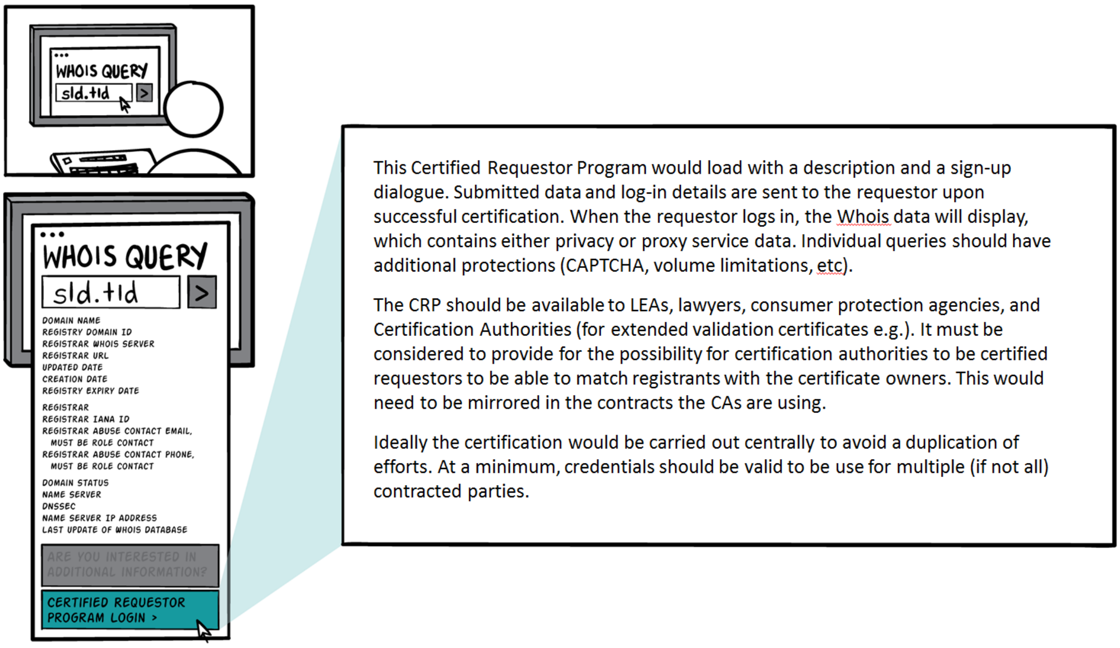
Request can be based on performance of the contract as all registrants have accepted these policies, Art 6 I b GDPR. If the requestor provides information on their IP and additional information to substantiate the request, the data will be revealed.

Requests can be based on legitimate interest, Art. 6 I f GDPR. If the requestor provides information on their IP and additional info to substantiate the request, the data will be revealed.

IP lawyers can use the sign-up process similar to the LEA accreditation process.

Requestor will be provided with an anonymized e-mail address or input field from which messages can be passed on to the registrant e-mail address

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:



This Certified Requestor Program would load with a description and a sign-up dialogue. Submitted data and log-in details are sent to the requestor upon successful certification. When the requestor logs in, the Whois data will display, which contains either privacy or proxy service data. Individual queries should have additional protections (CAPTCHA, volume limitations, etc).

The CRP should be available to LEAs, lawyers, consumer protection agencies, and Certification Authorities (for extended validation certificates e.g.). It must be considered to provide for the possibility for certification authorities to be certified requestors to be able to match registrants with the certificate owners. This would need to be mirrored in the contracts the CAs are using.

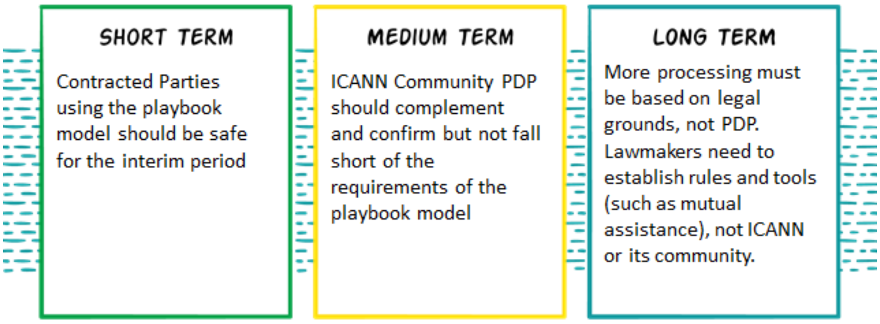
Ideally the certification would be carried out centrally to avoid a duplication of efforts. At a minimum, credentials should be valid to be use for multiple (if not all) contracted parties.

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.

Outlook

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

Implementation of the playbook model in a timely fashion poses an additional challenge to all parties involved. Technical implementation needs to be 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.