eco Association of the Internet Industry

RA Thomas Rickert
Director eco Names & Number Forum

WIR GESTALTEN DAS INTERNET.
GESTERN. HEUTE. ÜBER MORGEN.

eco
VERBAND DER
INTERNETWIRTSCHAFT

General Data Protection Regulation

ALAC Capacity Building Seminar

WIR GESTALTEN DAS INTERNET.
GESTERN. HEUTE. ÜBER MORGEN.

eco
VERBAND DER
INTERNETWIRTSCHAFT

About eco

- eco is an Internet Industry Association
- more than 1000 members from more than 60 countries
- runs the DECIX
- eco‘s Names & Numbers Forum represents some 150 companies in the Domain Industry ranging from gTLD Registries (legacy and new), ccTLD Registries, Registrars, Consultants, Secondary Market

Starting date

- On May 25, 2018, the GDPR will enter into force, see Art. 99 GDPR.

- As it is a European Regulation, it will apply throughout Europe immediately from this date. Other than directives, a regulation does not need to be transposed into national law.

Goals of the GDPR

The purpose of the Regulation is to regulate data protection in a uniform manner throughout the EU, to give EU citizens better control over their personal data and regulate how controllers may use personal data. On the other hand, it shall ensure free flow of personal data within the EU and to regulate the export of personal data outside the EU.

Some of the main themes are

- increased transparency requirements (documentation, information and proof)
- increased data security requirements
- increased accountability, such as a requirement to report breaches
- right to be forgotten
- right to data portability
- privacy by default
- privacy by design

Lawfulness of processing (Art 6 (1) GDPR)

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

a. consent;
b. performance of a contract;
c. 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;

Lawfulness of processing (Art 6 (1) GDPR)

e. public interest or in the exercise of official authority vested in the controller;

f. 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.

Consent

- Consent is discussed as a potential way to make the existing system compliant. However, 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.

To whom is the GDPR applicable?

If your company is established in the EU, the GDPR is applicable, regardless of whether the data processing is taking place in the EU, see Art 3 (1) GDPR.

Further, according to Art 3 (2) GDPR, the Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, when the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b) the monitoring of their behavior as far as their behavior takes place within the Union.

A representative is required.

Exception, if processing is only occasional.

Sanctions

The GDPR contains an extensive catalogue of administrative fines for violations of the various obligations.

Depending on the breach, the GDPR provides for fines up to EUR 10,000,000 or 2% of global annual turnover (e.g. in case of not appointing a representative) or up to 20,000,000 or 4% of annual global turnover (e.g. in case of violating Art. 5, 6 or 7 GDPR), depending on the violation.

According to Art. 58 (2) GDPR supervisory authorities can impose further sanctions such as skimming of profits, imposing a temporary or definitive limitation including a ban on processing or ordering the controller or processor to bring processing operations in compliance with the provisions of the GDPR.

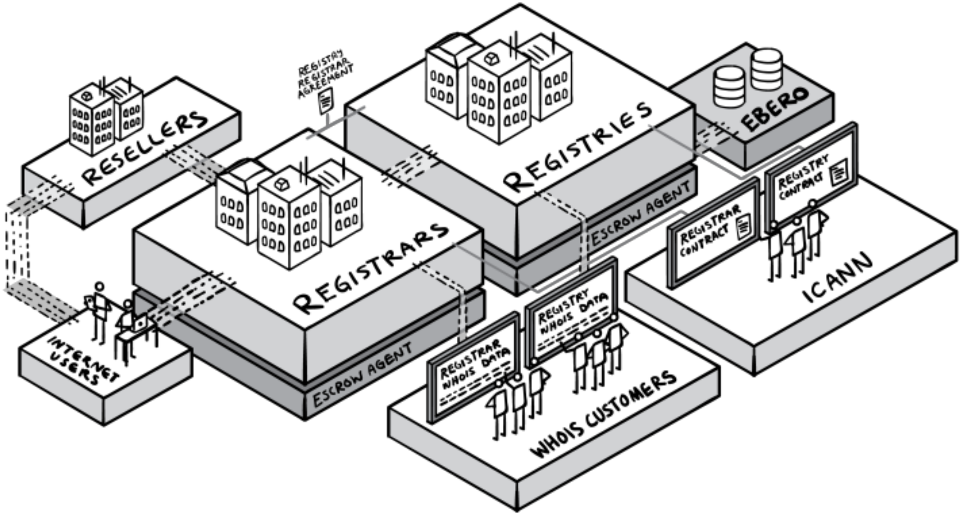
- The ICANN process
  - Contratcual compliance / interim phase
  - Long term / community process

  - ICANN has published models
  - eco has submitted the GDPR Domain Industry Playbook
  - https://www.icann.org/resources/pages/gdpr-legal-analysis-2017-11-17-en

- Problems with the proposed models are, amongst others:
  - Focus on disclosure of data vis Whois only
  - No analysis of the collection part
  - Baseline for all models is that all data elements currently collected will be collected
  - Baseline for all models is that data can travel from the registrar to the registry as a default

Here comes an outline of the eco Playbook model:

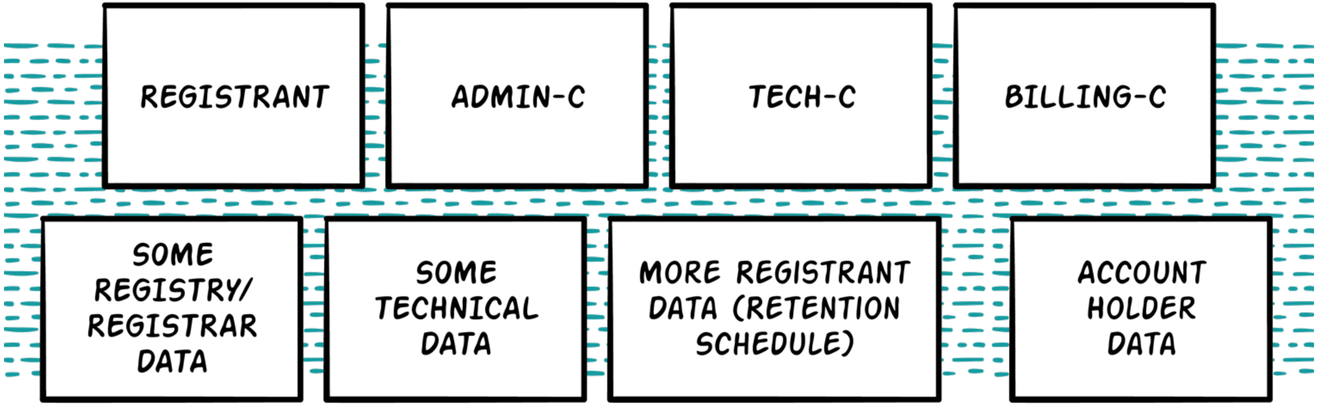
JOURNEY of DATA



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

- Note: The playbook discusses processing, but not transfers to entities outside the EU. That needs to be reflected all the way through, though. (p.12)

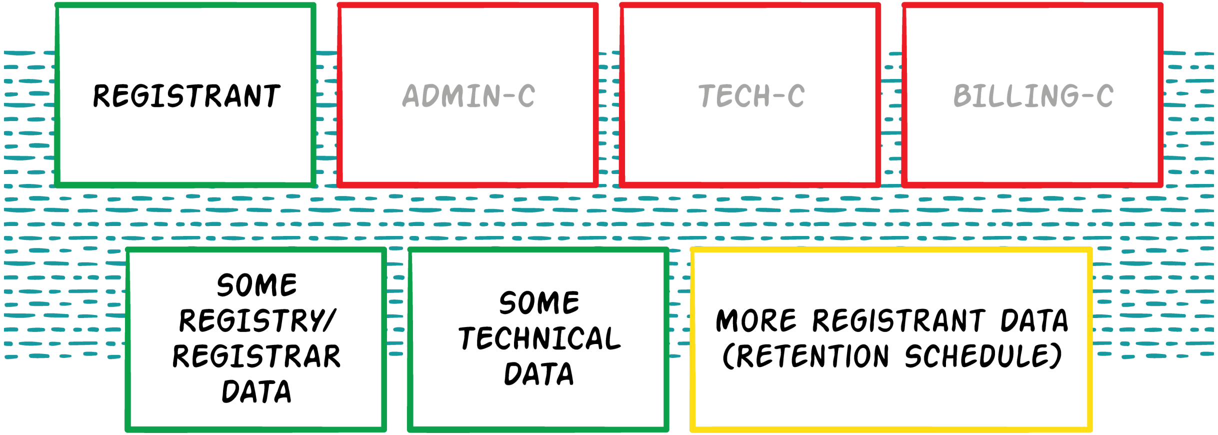
- Data elements currently used


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

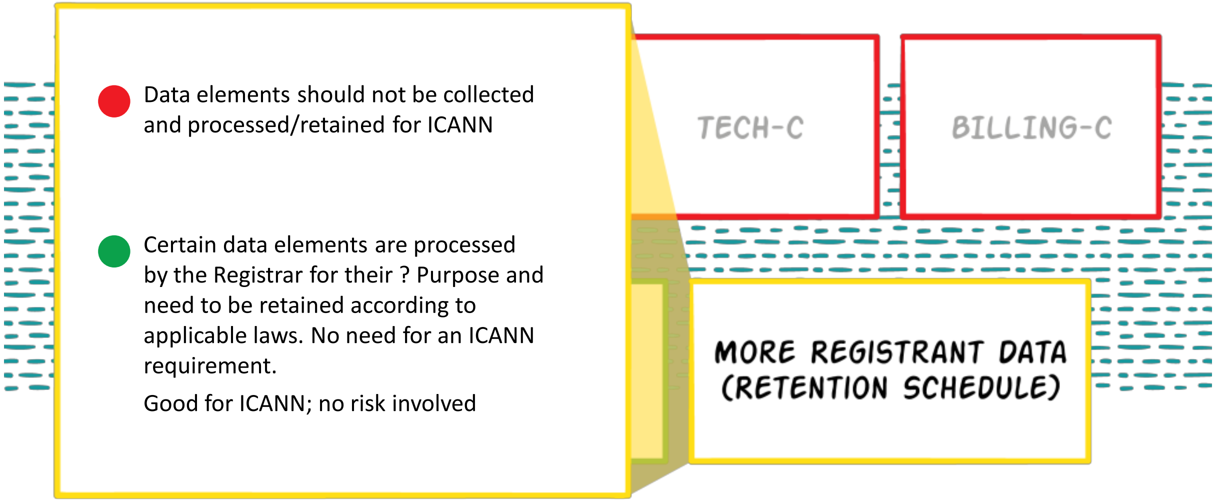
- We make a distinction between two scenarios:

  - Registry has no special requirements
  - Registry has special requirements such as Nexus, Elibibility, Local Presence requirements

- Registry has no special requirements, data at the registrar level


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

Basic Setup: Data Risk Level 1 > Registrar

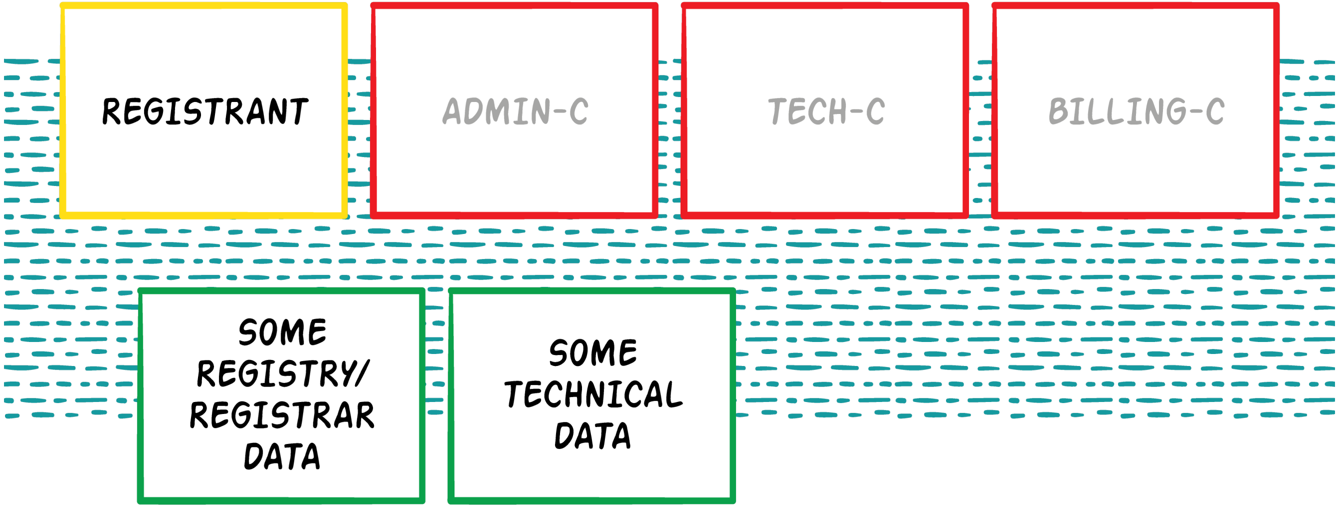


🔴 Data elements should not be collected and processed/retained for ICANN

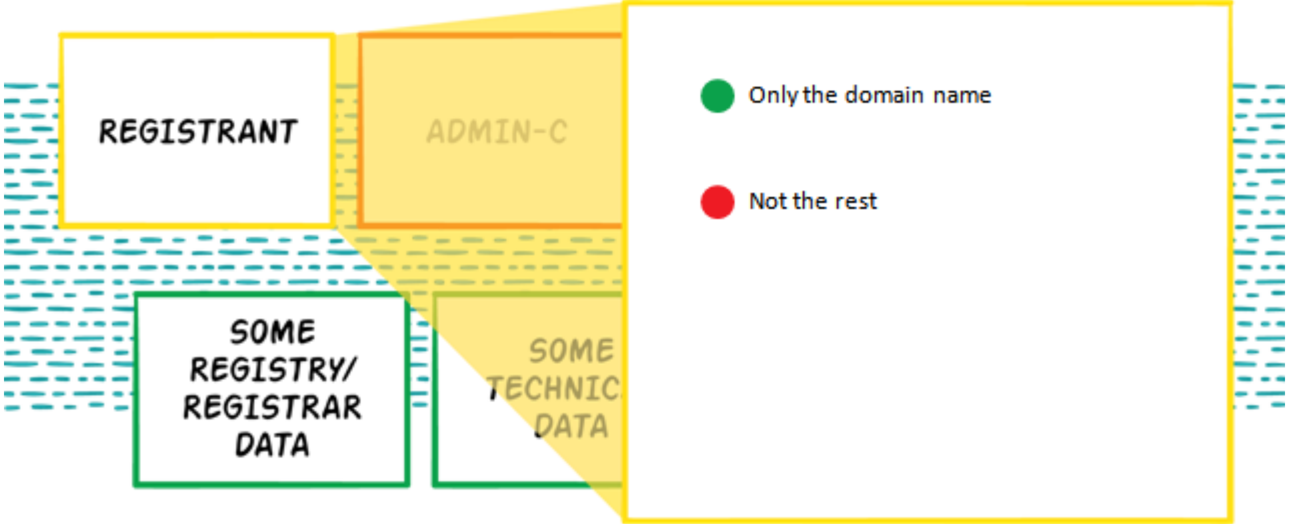
🟢 Certain data elements are processed by the Registrar for their ? Purpose and need to be retained according to applicable laws. No need for an ICANN requirement.

Good for ICANN; no risk involved

- DRL1 – Data at the registry level



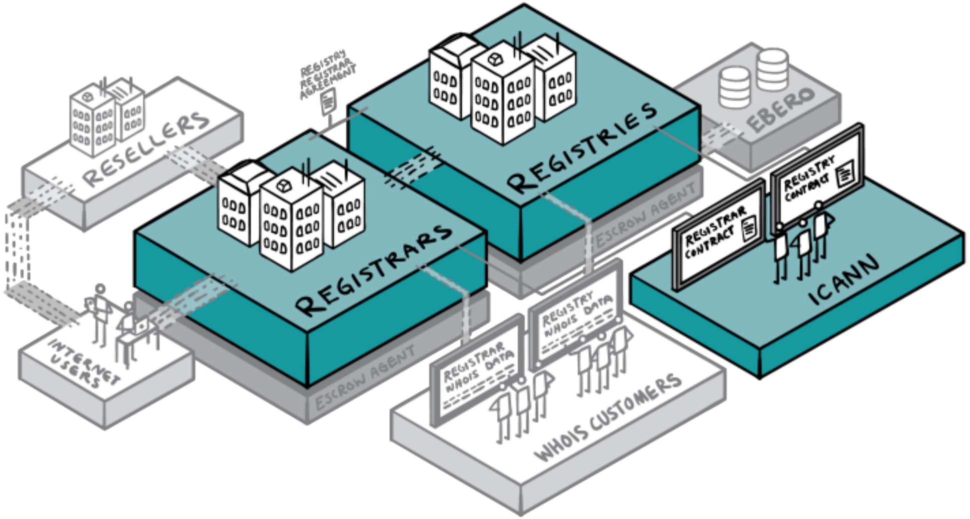
Basic Setup: Data Risk Level 1 > Registry



🟢 Only the domain name

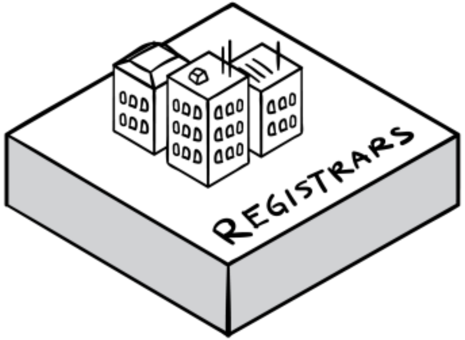
🔴 Not the rest

Journey of Data Joint Controllers: Data Risk Level 1



● Controller

Can the Registrar add data elements?



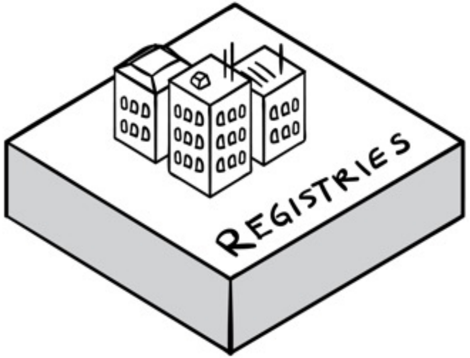
YES!

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

Registry has special requirements

Can the Registry add data elements?

YES!



DRL1
- Nexus
- Eligibility
- Admin-C Local Presence

DRL2
- Security Checks?

DRL3
- ???

DRL2 - Transfer of data to the registry

- Security checks
- Central management (???)
  - analogy of trademark databases
  - Thick Whois PDP discussion (related, but more in DLR1 if applicable)
- DLR2 processing should not be required and enforced by ICANN

DRL3 – processing based on consent

- Not a recommended solution for the reasons given above
- No prohibited, though
- Might be desired by registry operators for „trusted zones“ to allow for easier check by registrants whether or not the registrant is the trusted entity

Disclosure of Data

General considerations

- Privacy and Proxy services should remain untouched
- No justification for public WHOIS system under GDPR
- Every disclosure of data or access to data from a closed WHOIS needs a legal ground under the GDPR.
- **A closed system means a paradigm shift for both controllers and requesting parties!**
- **We need to go through the legal basis for different types of disclosure requests**

Art. 6 (1) b. – Performance of a contract

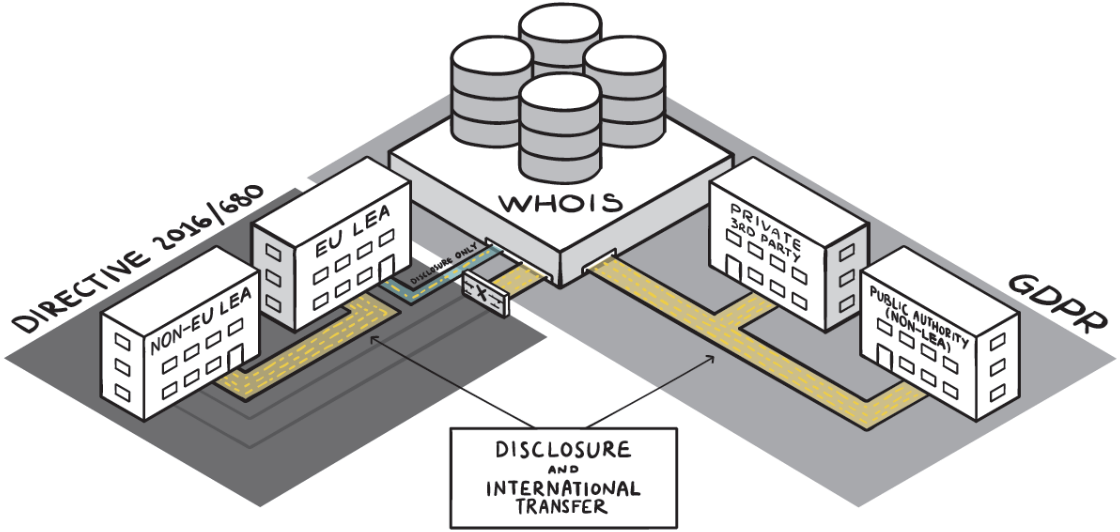
Contractual basis of domain registration contains provisions to certain conflict resolution systems. Data disclosure in terms of these systems, namely

- Uniform Domain Name Dispute Resolution (UDRP)
- Uniform Rapid Suspension Systems (URS)

remains untouched and is neccessary to perform a contract and justyfied by Art 6 (1) b.

Art. 6 (1) c. – Compliance with legal obligation

- Serves as legal basis for disclosure to public sector (e.g. Law Enforcement Agencies)
- Requires corresponding legal basis in the **laws of the EU or ist member states**
- No legal provisions of third party countries


WHOIS
DIRECTIVE 2016/680
EU LEA
NON-EU LEA
DISCLOSURE ONLY
PRIVATE 3RD PARTY
PUBLIC AUTHORITY (NON-LEA)
GDPR
DISCLOSURE AND INTERNATIONAL TRANSFER

Art. 6 (1) f. – Legitimate interests.

- Can not serve as a legal ground for disclosure to third country authorities.
- Domain registration must not be reduced to the use of a domain addresses, but registries / registrars are also serving the functionality and availability of a key global infrastructure. Data use or disclosure for security purposes should therefore basically be justifyable under the legitimate interest.

Legitimate interests

- Balancing of interests
- Neccessity of data processing
- Right to object
- 3rd parties interests

3rd party group	3rd party interest	Criteria for disclosure	Data to be disclosed
(IPR) attorneys	Legal action against alleged (IP) law infringements	• proof of bar admission / credible information of law infringement	DRL 1
Consumer protection associations	Legal action against consumer protection laws	• proof of entitlement / credible demonstration of consumer protection law	DRL 1
Certification authorities		• proof of operating certification process / request for certification by registrant	DRL 1
Other?			

Certification process for public authorities.

- Goal: replacing of a case-by-case assessment
- Safeguards by strict restrictions, purpose limitations, technical measures and documentation.

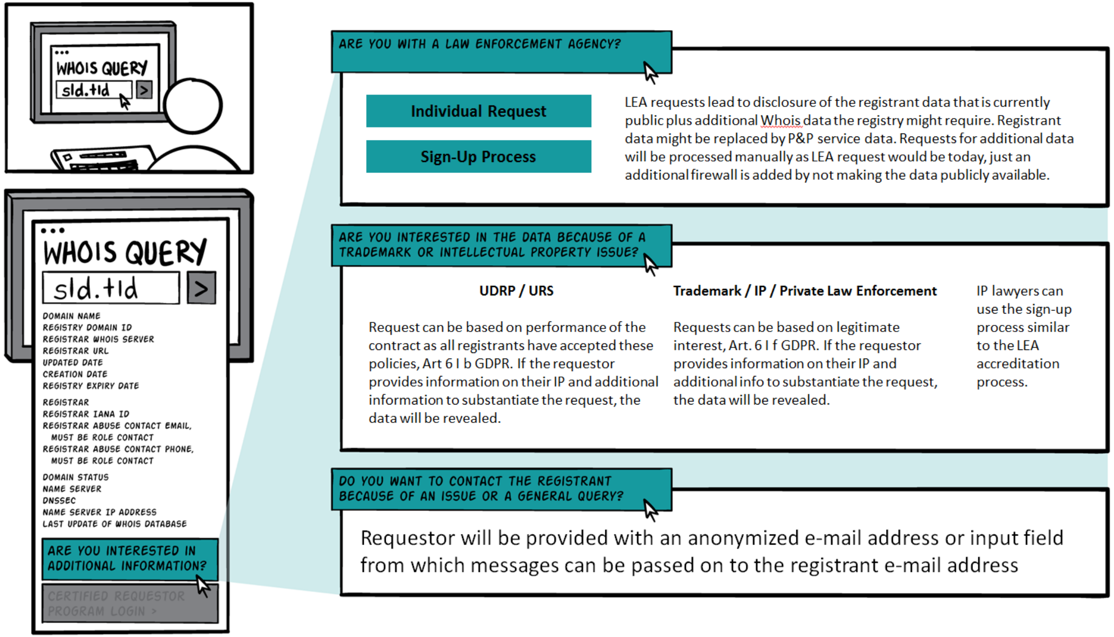
Certification process for private 3rd parties.

- Limitation to third parties according to table above.

- Safeguards: Provide evidence on respective role (e.g. attorneys ID card), filing by authorized persons; no mass data inquiries or for marketing purposes; no transferring to third parties, etc.

- Further protection from impact to data subject by limitation of inquiries; localization of request; use of CAPTCHAs.

Logical structure of Disclosure process I



ARE YOU WITH A LAW ENFORCEMENT AGENCY?

Individual Request

Sign-Up Process

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.

ARE YOU INTERESTED IN THE DATA BECAUSE OF A TRADEMARK OR INTELLECTUAL PROPERTY ISSUE?

UDRP / URS

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.

Trademark / IP / Private Law Enforcement

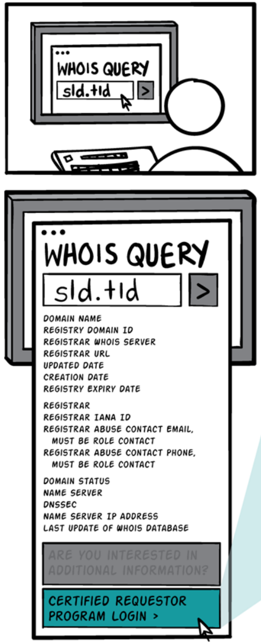
Requests can be based on legitimate interest, Art. 6 I f GDPR. If the requestor provides information on their IP and additional info to substantiate the request, the data will be revealed.

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

DO YOU WANT TO CONTACT THE REGISTRANT BECAUSE OF AN ISSUE OR A GENERAL QUERY?

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

Logical structure of Disclosure process II



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.

Proposal for a Trusted Data Clearinghouse (TDC).

- Procedure for processing information requests will entail high organizational effort for both the requesting party and controller.
- An expertly qualified and trustworthy instance could act as information broker an coordinate access to relevant data.
- A communication tool could provide access to certain non-certified requestors, given a legitimate interest can be assumed.