eco GDPR Domain Industry Playbook

Public Consultation

Brussels, Dec. 11, 2017

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

About eco

- Close collaboration with other associations
  - EuroISPA, Board
  - CENTR, observer
  - Internet Infrastructur Coalition (i2c) – special program with memership bundle

Background on the playbook

- Fragmentation in the industry should be avoided
- Discussions focused too much on disclosure (Whois)
- No holistic analysis for compliance
- Someone needed to take the initiative
- We chose to offer help and got a lot of support
- Not only for members, but beyond

We can….

- only do things such as the playbook if members want us to
- ony make this successful if YOU chime in and work with us
- only pay for such projects, if you become a member, book the membership bundle with i2c or otherwise financially contribute

PLEASE reach out to us or Lars (lars.steffen@eco.de) for info and answers to your questions.

The ICANN predicament

- ICANN‘s policy development is bottum-up consensus driven based on the multi-stakeholder model
- GDPR is a compliance issue and not at the disposal of the community
- ICANN has therefore broken the work down into two work streams
  - Contractual compliance phase with enforcement waiver
  - Policy development phase

Our approach

- Focusing on solving the contractual compliance issue, yet being transparent about our work
- Providing the baseline for the policy work
- 4 Phases
  - Small drafting team puts something on paper ✔
  - Consultation with experts from contracted parties ✔
  - Sharing the proposal ✔
  - Public Consultation and finalizing draft

Today‘s agenda

- Presentation of the proposal
- Discussion of the proposal
- Timing and priorities
- ICANN‘s latest post of criteria
- Conclusion and next steps

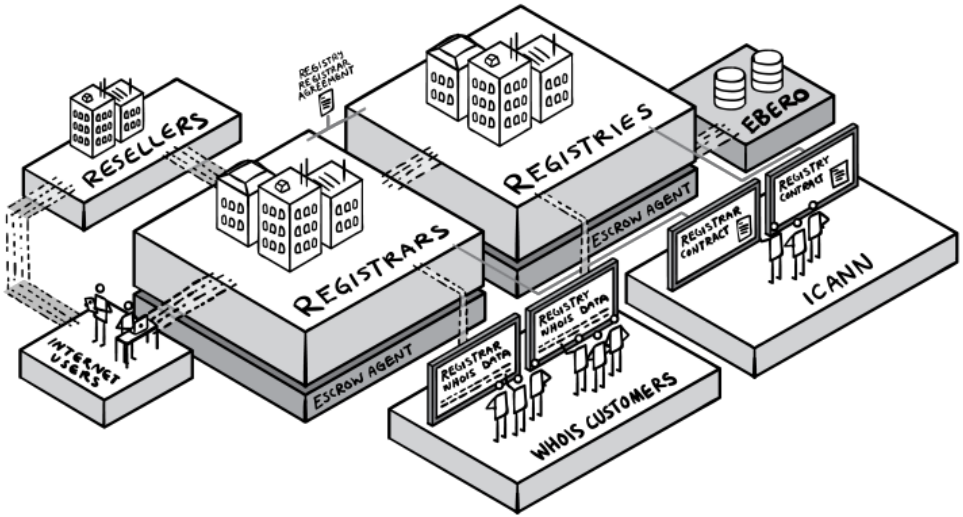
Structure of the Playbook

A. Introduction / Scope
B. Processing of data for domain registrations and maintaining domain registrations
C. Disclosure of data
D. Outlook

Structure of the Playbook

A. **Introduction / Scope**
B. Processing of data for domain registrations and maintaining domain registrations
C. Disclosure of data
D. Outlook

Journey of Data



- Principle of data minimization (p.7)
- Model based on how data can be processed in a legally compliant fashion (p.8).
- What is processing? (p.8)
  - 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.

- What is lawful processing? (p.8)
- (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;

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.

- A layered model (p.11)
- DRL 1 – Low risk – Performance of a contract
- DRL 2 – Medium risk – Legitimate interest
- DRL 3 – High risk – Consent

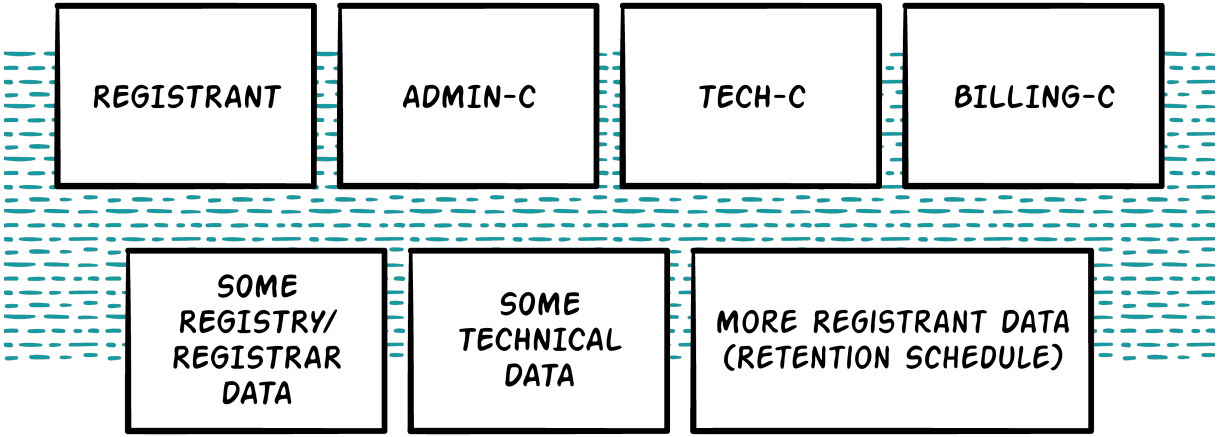
- Note: The playbook discusses processing, but not transfers to entities outside the EU. That needs to be reflected all the way through, though. (p.12)

- The term “risk” might too negative, better talk about compliance only?

Structure of the Playbook

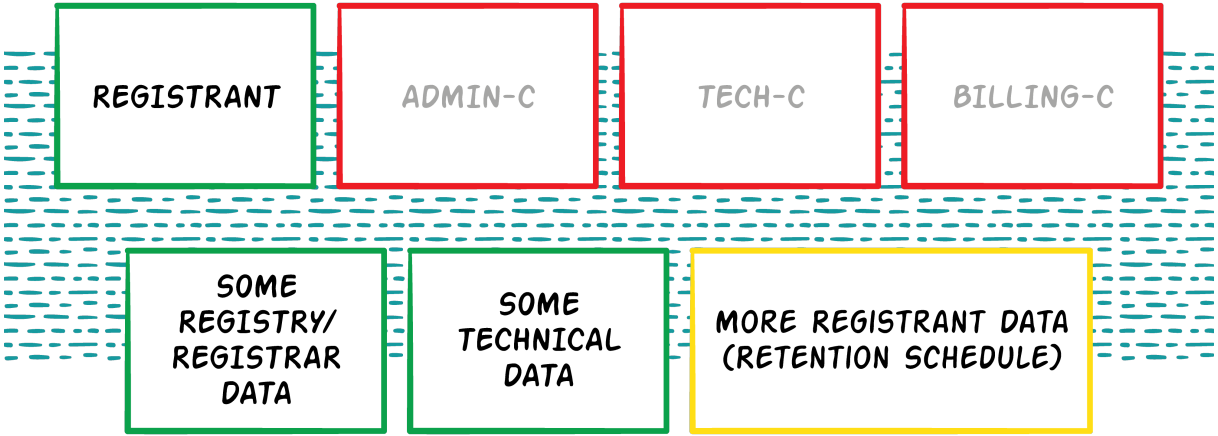
A. Introduction / Scope
B. Processing of data for domain registrations and maintaining domain registrations
C. Disclosure of data
D. Outlook

- Data elements currently used (p.14, 18)



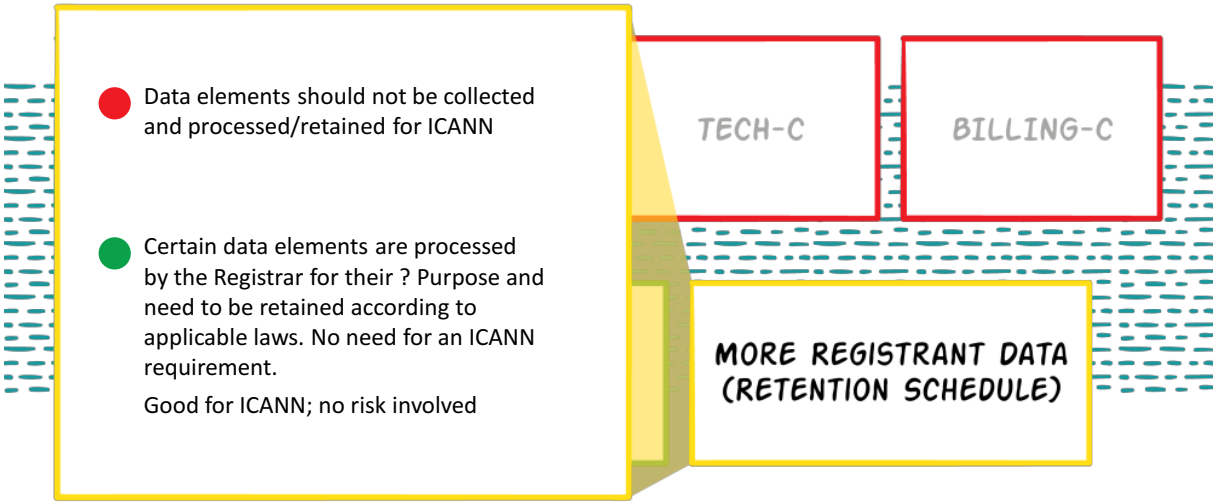
- We make a distinction between two scenarios:
    - Registry has no special requirements
    - Registry has special requirements such as Nexus, Elibibility, Local Presence requirements

- Registry has no special requirements, data at the registrar level (p.19)



- Registration data – ok
- Q: Distinction between natural and legal persons
- Admin-C, Tech-C, Billing-C – no
- Account holder data and data according to the data retention specification – no, but
  - as required to fulfill the contract
  - as required to be collected and retained by appliable laws
  - should not be an ICANN requirement
- Non PII – no changes!
- PII from Rr/Ry staff – no changes, parties should take care of that.

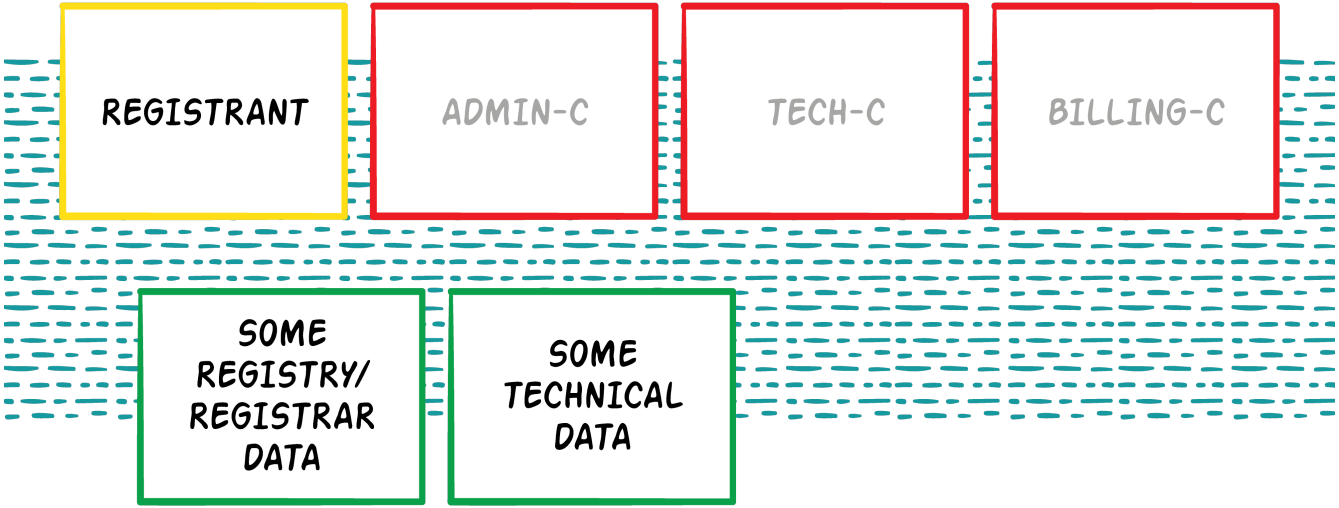
Basic Setup: Data Risk Level 1 > Registrar



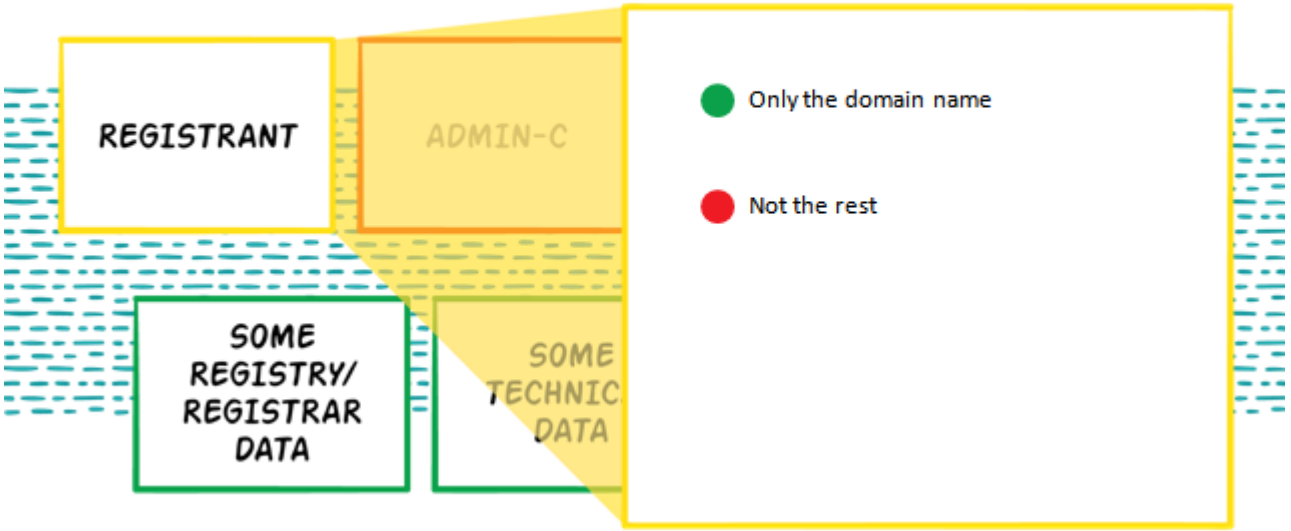
- Reasons:
  - Contract processing
  - Contactability
  - Transfers
  - Handling abuse reports
  - Ownership status

- Where the registration fails, the processing is still covered

- DRL1 – Data at the registry level (p.26)



Basic Setup: Data Risk Level 1 > Registry

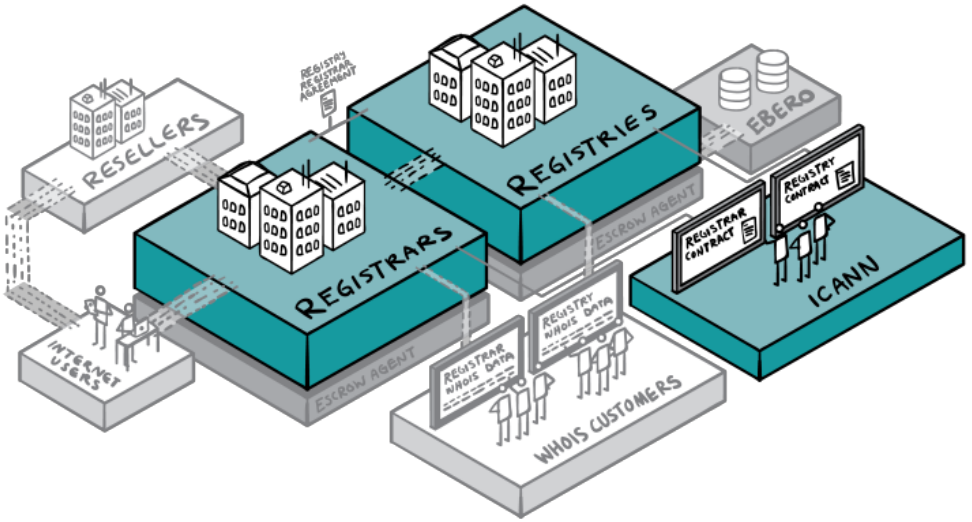


From data protection aspects, only the domain name is relevant for the registry as potentially personal data.
However, there has been a policy development process including all ICANN stakeholders confirming by way of a consensus policy that is binding for all contracted parties, that a thick Whois model 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. (p.27)

Responsibilities: Definitions Art. 4 no. (7) and no. (2) GDPR (p.30)

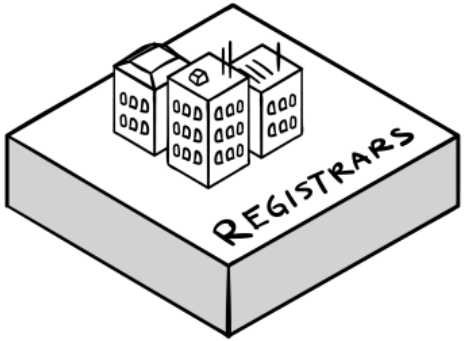
Controller is the person that alone or jointly with others determines the purpose and means of processing. Processing, in turn is "a*ny operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization,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

Journey of Data — Joint Controllers: Data Risk Level 1



Controller

Can the Registrar add data elements?

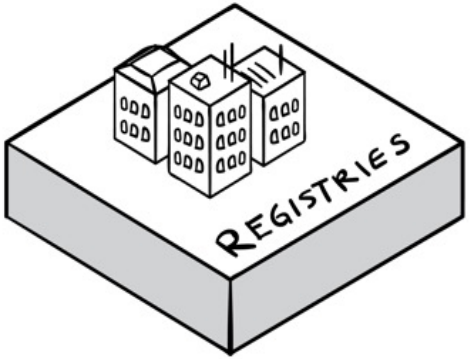


YES!

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

Registry has special requirements (p.37)

Can the Registry add data elements?



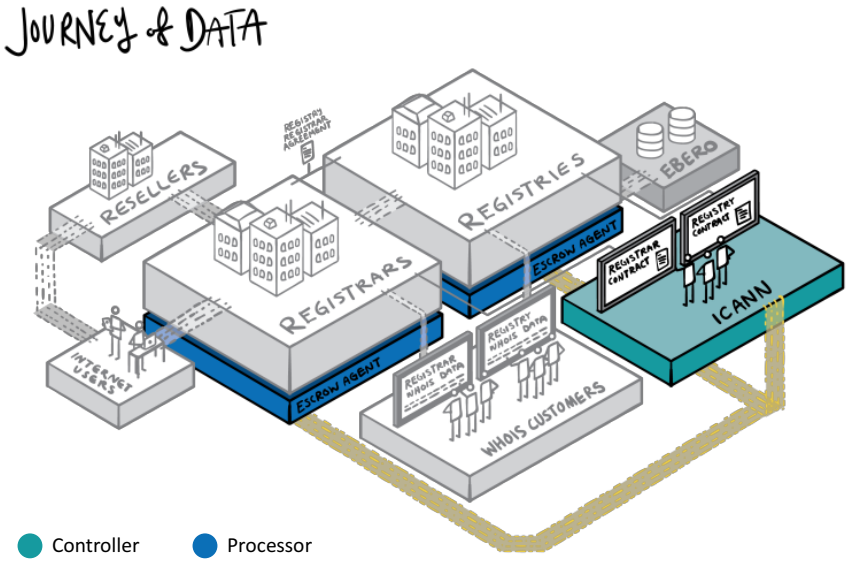
YES!

DRL1
- Nexus
- Eligibility
- Admin-C Local Presence

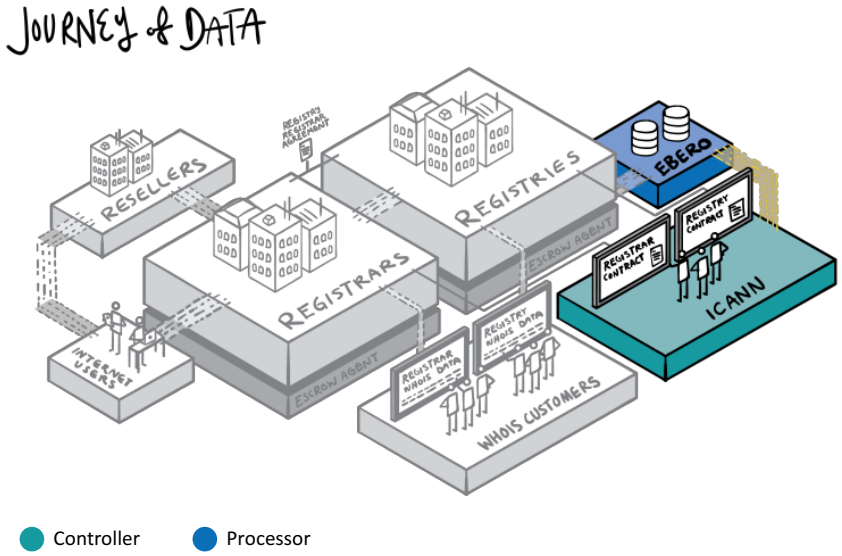
DRL2 · Security Checks?

DRL3 · ???

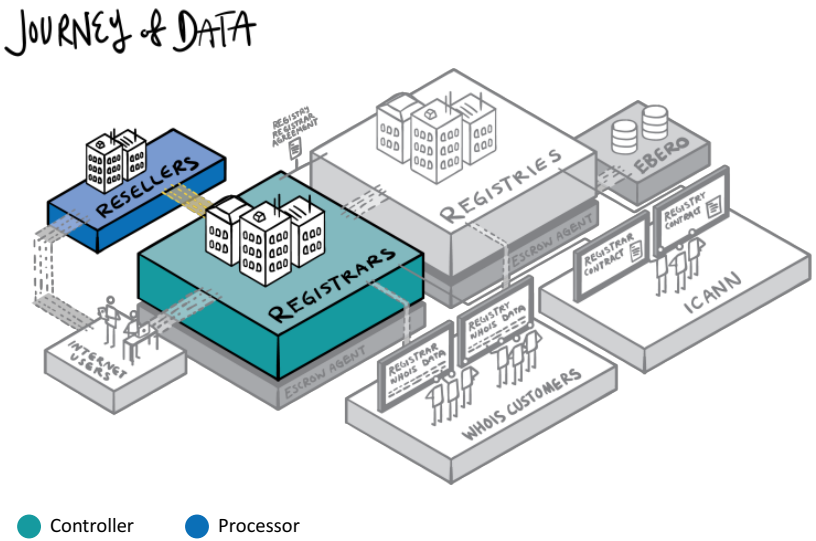
Escrow (p.39)


JOURNEY of DATA
RESELLERS
REGISTRIES
EBERO
REGISTRARS
ESCROW AGENT
ESCROW AGENT
REGISTRAR CONTRACT
REGISTRY CONTRACT
ICANN
REGISTRAR WHOIS DATA
REGISTRY WHOIS DATA
WHOIS CUSTOMERS
INTERNET USERS
Controller
Processor

EBERO (p.41)


JOURNEY & DATA
RESELLERS
REGISTRIES
REGISTRARS
EBERO
ICANN
REGISTRY CONTRACT
REGISTRAR CONTRACT
ESCROW AGENT
ESCROW AGENT
INTERNET USERS
REGISTRAR WHOIS DATA
REGISTRY WHOIS DATA
WHOIS CUSTOMERS
Controller
Processor

Resellers (p.44)



DRL2 - Transfer of data to the registry (p.45)

- 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 (p.48)

- 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

Structure of the Playbook

A. Introduction / Scope
B. Processing of data for domain registrations and maintaining domain registrations
C. Disclosure of data
D. Outlook

Legal grounds and criteria for disclosure

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

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

Art. 6 (1) f. – Legtimate interest, except overriding interests of data subject

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.

Page 52
Playbook

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

Guidelines for proper provisions. They shoud specify

- which general conditions govern lawfulness of processing
- which types of data are subject to processing
- which data subjects are concerned
- to which entities and purposes data may be disclosed
- Purpose limitation
- Retention periodes
- Processing operations in use.

Page 54
Playbook

In order to disclose data in a GDPR compliant way, check for

- Letterhead of respective organisation
- Signature of authorized represantative
- Legal basis referred to
- Affirmation, that data will only be reviewed in context of statitory competences.

Page 54
Playbook

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.

Page 55
Playbook

Legitimate interests

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

Page 56
Playbook

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?			

Page 58
Playbook

Certification process for public authorities.

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

Page 60
Playbook

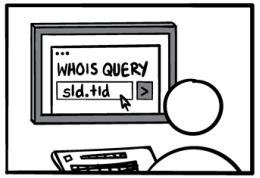
Certification process for private 3rd parties.

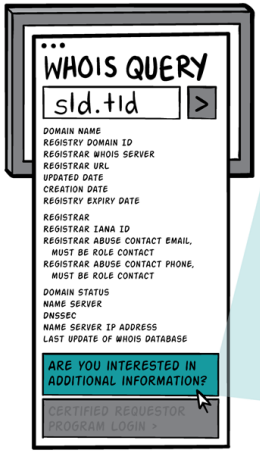
- Limitation to third parties according to table above.

- 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.

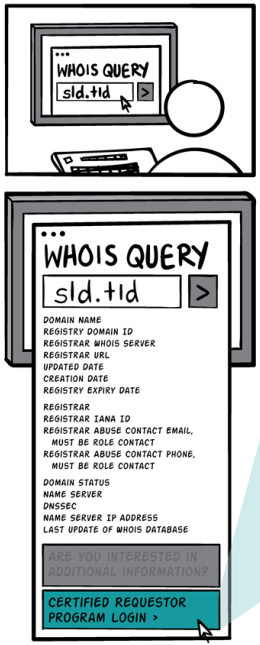
IP lawyers can use the sign-up process similar to the LEA accreditation process.

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

Page 63
Playbook

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.

Page 63
Playbook

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.

Page 64
Playbook

Part C – Disclosure of Data

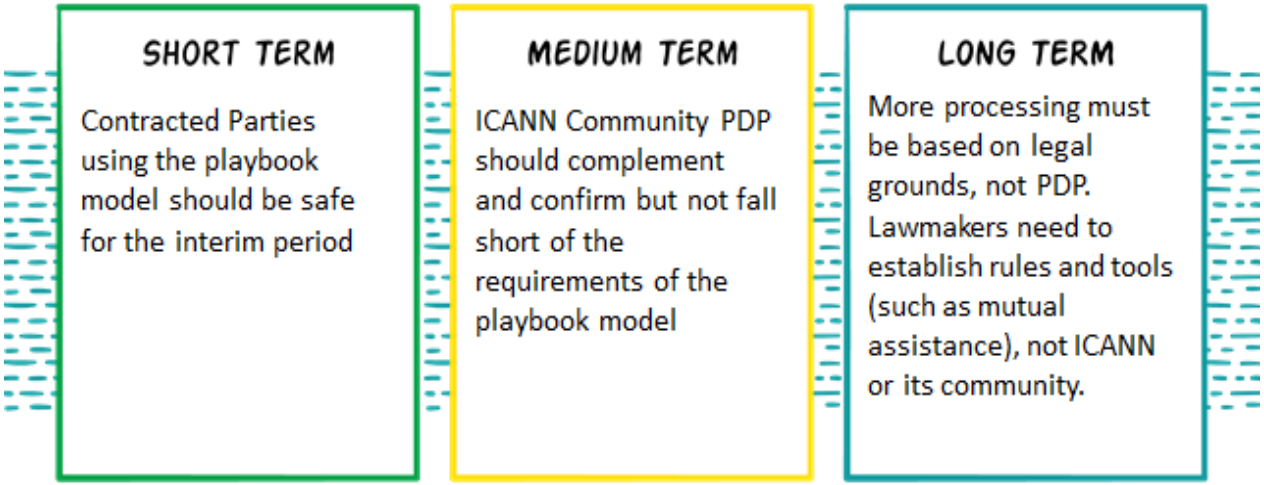
General considerations

- 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!**

Page 59
Playbook

Structure of the Playbook

A. Introduction / Scope
B. Processing of data for domain registrations and maintaining domain registrations
C. Disclosure of Data
D. Outlook



Page 66
Playbook

Questions / Comments? – Some rules:

- We will discuss chapter by chapter. Stay on topic, please!
- Please state your name and afiliation!
- Keep your statement brief (2 min max.)
- If you have a question in the chat, please mark it with „QUESTION“ so we can identify it as such.

- NOTE: The session is recorded.