

## GAC PUBLIC SAFETY WORKING GROUP (PSWG)

### PSWG Intersessional Meeting – 12-13 February 2018 Chair's Conclusions

#### I. OBJECTIVES

---

The Public Safety Working Group of ICANN's Governmental Advisory Committee (GAC), together with cybercrime experts from 25 EU Member States and 3 associated States participating in the EMPACT Programme (European Multidisciplinary Platform against Criminal Threats), met to address the the impact of the impending reform of the Whois service and protocol, which may entail loss of public access to Whois data. This reform is set to address long-standing data protection concerns, which have become more acute with the coming into effect of the EU General Data Protection Regulation (GDPR) in May 2018.

While the focus was on Whois, this meeting was also an opportunity for law enforcement representatives to familiarize themselves with the activities of ICANN and how, within ICANN, law enforcement can influence the development of policies that are applied through contracts, across the domain industry. It also served to provide an introduction to the DNS abuse mitigation work of the GAC PSWG.

#### II. WHOIS IS CRITICAL FOR LAW ENFORCEMENT INVESTIGATIONS

---

The public availability of worldwide Whois data from which law enforcement agencies and other legitimate users have benefited for many years, has been the subject of concerns by data protection authorities since 2003. To better protect the privacy of domain name registrants, there is a plan to move to a "layered access" model where personal data (and as likely implemented, even some corporate data) will no longer be publicly accessible.

Several models under consideration in the ICANN community are proposing a wide range of solutions in terms of:

- data collection requirements (what data is collected from registrants of domain name)
- accessibility of data by third parties (including law enforcement among other legitimate users)
- retention of collected data (for maintenance of historical records in particular)

The GAC, the European Commission and the US Government have advised<sup>1</sup> ICANN to adopt solutions that preserve current legitimate uses of public Whois data to the maximum extent possible in compliance with data protection rules, while providing for swift and practical access to non-public data for law enforcement.

As illustrated by the German Federal Criminal Police Office (BKA) and Europol, domain registration data made available through the Whois system is critical to law enforcement investigations. While the quality and accuracy of such data is uneven, it is almost always instrumental in generating investigative leads and ultimately attributing crime. Participants also identified the value of Whois data to identify victims of cybercrime. Examples cited included domain owners in cases of hijacked domains (using past Whois data) and in cases of compromised domains (using present-day Whois data). Law enforcement also referred to the use of Whois to identify a child victim of sexual abuse which was rescued using information on the domain name registrant committing the abuse and sharing images of it.

---

<sup>1</sup> See actual contributions from the [GAC](#), the European Commission ([commissioner's letter](#), [comments](#)) and the [US Government](#).

### III. LAW ENFORCEMENT NEEDS TO RETAIN FULL ACCESS TO WHOIS DATA, WHILE PROVIDING APPROPRIATE DATA PROTECTION SAFEGUARDS

---

Participants in the meeting have identified specific needs and challenges that need to be addressed in the implementation of the new GDPR-compliant Whois system, including:

- **Scope of personal data collection:** investigations show that all data elements can prove valuable, while the data minimization and proportionality principles of the GDPR may require a reduction of the amount of data available
- **Practicability of access to non public data:** modalities of access to non-public data need to be consistent across all Top-Level Domains (TLDs) and commensurate with high rates of access needed by law enforcement for specific types of investigations (e.g. botnets)
- **Cross-referencing, search capabilities and historical records of Whois data:** law enforcement agencies need replacements for third-party services (such as those available from Domain Tools) that used to rely on the public availability of all Whois data. This includes new features of Whois, as well as appropriate data retention specifications (including for changes of registration information).
- **Confidentiality of requests for non-public data:** while law enforcement generally recognize the greater trustworthiness of registries compared to registrars, requests for non-public data by law enforcement should not be identifiable by concerned parties in order to avoid compromising investigations
- **Cybersecurity firms access:** trusted partners in cybercrime investigations need to retain access to full data
- **National accreditation of law enforcement agencies to access gated data:** national accreditation would be preferable to a centralised accreditation system as it is best left to national governments to assess which law enforcement agencies should be granted which competences. However, this could present challenges because each nation has a distinct set of law enforcement entities. Some nations have thousands of law enforcement entities at the federal, state, and local levels. Implementing such an accreditation system could take considerable, time, effort, and resources.

### IV. NEXT STEPS IN WHOIS COMPLIANCE WITH GDPR

---

The PSWG in collaboration with the GAC is preparing to assist in providing feedback and guidance regarding the selected model soon to be chosen by ICANN and implementation thereof.

To that effect, the PSWG is currently refining a set of Law Enforcement Requirements for a Future Layered Access Model which it has started discussing with interested parties in the industry and the technical community. Further outreach is planned to other parts of the community. These requirements could form a basis for discussions also with data protection and technical experts to determine data protection-compliant solutions and identify the most privacy-protective means of implementation.

## V. PSWG WORK PLAN AND OUTREACH

---

Law enforcement participants also discussed the workplan of the PSWG which lays out the future work for the period 2018-2019 in order to achieve its 4 strategic objectives:

1. Developing capabilities of the ICANN and Law Enforcement communities to prevent and mitigate abuse involving the DNS as a key resource
2. Ensuring continued accessibility and improved accuracy of domain registration information that is consistent with applicable privacy regulatory frameworks
3. Building effective and resilient PSWG operations
4. Developing participation in PSWG Work and ensuring appropriate stakeholder input

A number of opportunities for improving the outreach of the PSWG to law enforcement practitioners have been identified, including:

- Informing about opportunities for contributions to ICANN public comments
- Offering webinar on issues of interest to law enforcement as well as material explaining the role of the PSWG in ICANN's multi-stakeholder model
- Creating a law enforcement Internet governance mailing list to support the involvement of law enforcement representatives that are not yet members of the PSWG
- Creating a monthly PSWG newsletter that provides updates on current activities and issues of interest
- Identifying opportunities for input to PSWG work

## VI. LIST OF PARTICIPANT COUNTRIES (ALPHABETICAL ORDER)

---

|                |                 |
|----------------|-----------------|
| Austria        | Italy           |
| Belgium        | Luxemburg       |
| Bulgaria       | The Netherlands |
| Canada         | Norway          |
| Cyprus         | Poland          |
| Czech Republic | Portugal        |
| Denmark        | Romania         |
| Estonia        | Slovenia        |
| Finland        | Spain           |
| France         | Sweden          |
| Germany        | Switzerland     |
| Greece         | United Kingdom  |
| Hungary        | United States   |
| Ireland        | Zambia          |

## ANNEXED DOCUMENTS

---

1. Agenda of day 1 of the meeting (12 February 2018)
2. Agenda of day 2 of the meeting (13 February 2018)
3. Draft Proposal for minimum requirements for LEA access to a future layered access model to non-public domain registration data (as of 9 February 2018)
4. Draft PSWG Work Plan (as of 26 February 2018)
5. PSWG presentation material (selected meeting slides)
6. Presentation of ICANN (meeting slides)



EUROPEAN COMMISSION  
DIRECTORATE-GENERAL MIGRATION and HOME AFFAIRS

Directorate D: Security  
Unit D.4 : Cybercrime

Brussels, 5 January 2018

[HOME.D.4/CBB](#)

Members of the ICANN GAC PSWG  
Members of the EMPACT Priority on Cyber Attacks

**Subject: GAC PSWG intersessional meeting on the future of WHOIS and DNS abuse mitigation**

Dear PSWG members, dear EMPACT participants,

For many years, law enforcement agencies (LEAs) have relied on WHOIS services, which provide publicly available domain name registrations information. The WHOIS is a key tool to investigate and attribute crime. Data Protection Agencies have long identified issues with the public availability of personal data contained in the WHOIS; nonetheless, the ICANN community has not yet managed to come to agreement on any replacement policy, and LEA access to such data has been largely unaffected. This is now set to change fundamentally in the coming months, before the entry into effect of the EU GDPR on 25<sup>th</sup> May 2018.

To discuss the latest developments around WHOIS and DNS abuse, their impact on public safety stakeholders, and possible measures to mitigate this impact, the European Commission would like to invite you to **Brussels, Belgium**, for an intersessional ICANN Governmental Advisory Committee Public Safety Working Group (GAC PSWG) meeting which will take place on **12<sup>th</sup> February 2018**. This workshop will bring together members of the GAC PSWG and representatives of EU Member States' law enforcement agencies participating in the EMPACT priority on cyber attacks; it should result in a better understanding of the needs of these two groups and concrete measures to take them into account. The language of the meeting will be English; no translation will be provided.

We will also use this opportunity to review progress on measures for prevention and mitigation of Domain Name System abuse and identify next steps, as well as to discuss the work plan and outreach for the GAC PSWG. This should also extend to how better to integrate public safety stakeholders unable to participate in face-to-face ICANN meetings.

Please find enclosed the draft agenda of the day. If you intend to participate, please register until 18<sup>th</sup> January 2018 using the following form: <https://ec.europa.eu/eusurvey/runner/PSWG>.

The European Commission will reimburse one participant per EU Member State for EMPACT members and up to 15 members of the PSWG (topic leads have priority; the remaining reimbursements will be attributed according to the time of registration [first come, first serve]). Please do not make your own booking for travel or hotel; our contractor will be in touch with you to arrange your travel.

For the EMPACT participants, please note for your travel plans that Europol plans to organise a related workshop on 13 February in Brussels for which you may wish to stay on. Further information on this workshop will be provided by Europol directly.

Please contact our functional mailbox [HOME-NOTIFICATIONS-D4@ec.europa.eu](mailto:HOME-NOTIFICATIONS-D4@ec.europa.eu) for any questions regarding the registration or reimbursement.

We look forward to discussing these important issues with you and count on your numerous and active participation in the event.

Yours sincerely,



Cathrin BAUER-BULST  
Deputy Head of Unit  
Co-Chair, GAC PSWG

Encl.: Agenda of the workshop on 12<sup>th</sup> February 2018.

# PSWG Intersessional Meeting on 12<sup>th</sup> February 2018

## Agenda

Time: Monday, 12<sup>th</sup> February 2018, 10:00 h to 18:00 h.

Place: Albert Borschette Congress Center ([CCAB](#)), Room 1B, rue Froissart 36, 1040 Etterbeek.

Participants will have to undergo a security check which includes a visual inspection with X-rays.

| <b>Time</b> | <b>Issue</b>   | <b>Leader</b>  |
|-------------|--|--|
| 10:00 h     | Welcome and opening of the workshop  | Cathrin BAUER-BULST (EC)   |
| 10:10 h     | Presentation of the WHOIS model(s) received (and possibly chosen) by ICANN | TBD  |
| 10:30 h     | Needs of law enforcement (LE)  | Grégory MOUNIER (Europol)  |
| 11:00 h     | Coffee break   |  |
| 11:20 h     | Discussion of the model(s) and their fulfilment of LE needs (part 1)       | Cathrin BAUER-BULST (EC)/Laureen KAPIN (US FTC)                      |
| 12:50 h     | Lunch break  |  |
| 13:40 h     | Discussion of the model(s) and their fulfilment of LE needs (part 2)       | Cathrin BAUER-BULST (EC)/Laureen KAPIN (US FTC)                      |
| 14:40 h     | DNS abuse mitigation   | Iranga KAHANGAMA (US FBI)  |
| 15:40 h     | Coffee break   |  |
| 16:00 h     | PSWG Work Plan and Outreach  | Cathrin BAUER-BULST (EC)/Grégory MOUNIER and Sara MARCOLLA (Europol) |
| 18:00 h     | Closing  | Cathrin BAUER-BULST (EC)   |

The Hague, 25/01/18

EDOC#941193-v2

## AGENDA

### GAC PSWG-EMPACT meeting on the future of WHOIS and DNS abuse mitigation – Day 2: RDAP

|                |                  |             |            |
|----------------|------------------|-------------|------------|
| <b>Date(s)</b> | 13 February 2018 | Start: 9:00 | End: 13:00 |
|----------------|------------------|-------------|------------|

**Place**                    **DG HOME, Falcone/Borsellino on the ground floor of  
the LX46 building.**

**Participants**        **EUCTF delegates, Private Partners, DG HOME, ICANN  
EC3 staff**

| <b>Time</b>   | <b>Subject</b>                          | <b>Responsible</b>   |
|---------------|---|--|
| 09:00 – 09:10 | Welcome note and opening of the meeting | Gregory Mounier<br>EUROPOL<br>Cathrin Bauer-Bulst<br>DG HOME |
| 09:10 – 10:00 | Presentation of the RDAP pilot project  | Francisco Arias<br>ICANN                                     |
| 10:00 – 11:00 | RDAP Implementation - Verisign          | Marc Anderson<br>and<br>Rick Wilhelm<br>Verisign             |
| 11:00 – 11:30 | Coffee Break                            |  |
| 11:30 – 12:45 | Discussion: LEA requirements            | Tour de table  |
| 12:45 – 13:00 | Conclusion<br>End of meeting            | Gregory Mounier<br>EUROPOL                                   |



## Background paper

### Minimum requirements for LEA access to a future layered access model to domain registration data

#### 1. Aim

- To receive feedback from the EU law enforcement community on practical requirements for LEA access to non-public WHOIS information.
- To prepare the discussion with VERISIGN on the RDAP pilot programme on 13<sup>th</sup> February 2018.

Do you have experience using gated/layered access systems, e.g. on the basis of credentials assigned to you personally or to your organisation? Which requirements exist for your organisation? Could you please prepare comments on the minimum requirements proposed on page 3 (part 4)?

#### 2. Background

For many years, law enforcement agencies (LEAs) have relied on WHOIS services, which provide publicly available domain name registrations information to investigate and attribute crime online.

Data Protection Agencies have taken issue with the public availability of personal data contained in the WHOIS<sup>1</sup>; nonetheless ICANN policy related to WHOIS in gTLDs has not evolved significantly as the community did not manage to come to agreement on any replacement policy, and LEA access to such data has been largely unaffected.

This is now set to change fundamentally with the entry into effect of the EU GDPR on 25 May 2018. A growing body of legal opinions<sup>2</sup> recognizes that collection and publication of personal data contained in the WHOIS database is unlawful and that compliance with GDPR will likely involve reducing the number of data elements collected and implementing purpose-based access to differentiated subsets of the remaining registration data, also known as **layered access**.

As a consequence, while the legitimacy of law enforcement access to registration data, including personal data, for investigations purposes is generally not challenged, LEA access to such data will be affected, both from a practical and from a legal perspective. Practically speaking, there will be fewer data elements and therefore fewer leads available. Cross-referencing data elements across different registrations, e.g. to identify which other domains a bad actor may have registered using the same information, would likely no longer be possible.

Currently under consideration are the following models:

---

<sup>1</sup> <https://www.icann.org/en/system/files/correspondence/falque-pierrotin-to-chalaby-marby-06Dec17-en.pdf>

<sup>2</sup> <https://www.icann.org/en/system/files/files/gdpr-memorandum-part1-16oct17-en.pdf>; <https://gnso.icann.org/en/drafts/wsg-icann-memorandum-25sep17-en.pdf>

- a model where every WHOIS lookup would require an individualized request justifying the purpose for access, specific data elements sought, etc., possibly validated by a judge;
- a model where some form of authentication would be provided, allowing access for law enforcement by means of logins and passwords. Such access might be provided through a centralized clearinghouse logging access requests and verifying proportionality.

While such models are advantageous from a data protection perspective, they might create a number of challenges and risks for law enforcement. In particular, individualized access requests would be difficult to fathom in view of the fact that one cyber unit might make as many as 50,000 lookups a week. Tracking and tracing law enforcement activity might reveal sensitive data, potentially compromising investigations if revealed or illegally accessed.

In addition, while law enforcement access is not contested, it is unclear whether and how other relevant actors would maintain current levels of access. This concerns in particular cybersecurity authorities, private sector companies and academic researchers; consumer protection authorities, or IP right holders.

### 3. Recent developments<sup>3</sup>

Based on consultations with contracted parties, European data protection authorities, legal experts, and interested community stakeholders, ICANN proposed on 12 January 2018, **three potential interim compliance models** with ICANN agreements and policies in relation to the EU's GDPR.<sup>4</sup> **All three models introduce a variation on layered access to WHOIS data.** The variations of the three models revolve around geographic scope (EU-centric or global), scope of publication of data elements, and third party access to non-public data.

In line with GDPR requirements, ICANN defines five distinct purposes for the WHOIS system, including two specific purposes related to law enforcement needs and investigating cybercrime.

- Supporting a framework to address issues involving domain name registrations, including but not limited to: consumer protection, investigation of cybercrime, DNS abuse, and intellectual property protection; and*
- Providing a framework to address appropriate law enforcement needs.*

Regarding law enforcement access to non-public data, ICANN proposed three options:

- i) Self-certification of legitimate interest to be approved by each registry/registrar;
- ii) Certification programme to be developed in consultation with the GAC<sup>5</sup>;
- iii) Court order or legal requirement.

ICANN requested feedback on these interim potential compliance models by 29 January 2018. It intends to decide on and **publish a single model by mid-February 2018.**

---

<sup>3</sup> For an overview of the WHOIS reform issue please see p.11 of the Progress report.

<sup>4</sup> <https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf>

<sup>5</sup> [Governmental Advisory Committee of ICANN where all EU Member States are represented together with the European Commission: https://gacweb.icann.org/display/gacweb/GAC+Representatives](https://gacweb.icann.org/display/gacweb/GAC+Representatives)

This model will then serve as the standard for ICANN itself and for compliance with the WHOIS obligations under the Registrar and Registry contracts. In practical terms, it will be the one and only WHOIS model.

Among the many contributions received by ICANN, please note the following:

- **GAC Comments** (prepared by the PSWG): <https://www.icann.org/en/system/files/files/gdpr-comments-gac-icann-proposed-compliance-models-29jan18-en.pdf>
- **European Commission**: <https://www.icann.org/en/system/files/correspondence/avramopoulos-et-al-to-marby-29jan18-en.pdf>
- **United States**: <https://www.icann.org/en/system/files/files/gdpr-comments-usg-icann-proposed-compliance-models-29jan18-en.pdf>
- **UK NCA**: <https://www.icann.org/en/system/files/files/gdpr-comments-nca-icann-proposed-compliance-models-29jan18-en.pdf>
- **WIPO**: <https://www.icann.org/en/system/files/files/gdpr-comments-wipo-icann-proposed-compliance-models-29jan18-en.pdf>
- **Registrar Stakeholder Group**: <https://www.icann.org/en/system/files/files/gdpr-comments-rrsg-icann-proposed-compliance-models-29jan18-en.pdf>
- **A group of contracted parties (including Donuts, GoDaddy and others)**: <https://www.icann.org/en/system/files/files/gdpr-comments-contracted-icann-proposed-compliance-models-29jan18-en.pdf>
- **IPC**: <https://www.icann.org/en/system/files/files/gdpr-comments-ipc-icann-proposed-compliance-models-29jan18-en.pdf>
- **ECO Association**: <https://www.icann.org/en/system/files/files/gdpr-comments-eco-icann-proposed-compliance-models-29jan18-en.pdf>

#### 4. Proposal for minimum requirements for LEA access to a future layered access model to domain registration data:

In order to guarantee EU LEA access to essential WHOIS data, the PSWG is seeking to define a **set of minimum requirements** to guarantee timely LEA access to the appropriate elements of a **GDPR-compliant Registration Directory Services (RDS)**.

These minimum requirements might also be used as a joint input from the LEA community to the RDAP pilot program currently underway, testing a replacement protocol to WHOIS and which will allow for gated access<sup>6</sup>.

Because a layered access model implies **credentialing, authenticating** and **authorizing users** to access data that is not made public and may be hosted in foreign jurisdictions, below is a first series of draft minimum requirements for a future layered access model for discussions.

##### 2.1. Basic principles

---

<sup>6</sup> <https://community.icann.org/display/RP/RDAP+Pilot>

- The different **legitimate purposes** for which processing of registration data takes place should be clearly and explicitly set out in the policy rules that apply to such processing, from collection to storage and access of data.
- Processing of WHOIS data for law enforcement purposes, e.g. investigating and countering serious crime, fraud, consumer deception, intellectual property violations, and other law violations, constitutes a legitimate interest for processing of personal data. The processing of personal data shall be lawful and necessary for the performance of a task carried out by a competent authority for law enforcement purposes, in line with applicable data protection legal framework.
- These purposes should therefore **cover the legitimate need for law enforcement access to WHOIS data<sup>7</sup> to sustain public interests** such as cybersecurity; the stability, reliability and resilience of the network; preventing and fighting crime; protecting intellectual property rights, copyright and consumer rights; and other rights recognised in the domestic legal order.
- Registrants should be **informed in a clear and easily understandable manner** about these purposes and the related data processing when making, updating or extending registrations in line with the principle of transparency.

## **2.2. Necessary data elements**

- The model should give nationally-accredited actors, **access to all the WHOIS data necessary for the fulfilment of their task**, subject to the requirements that should be clearly stated in the processing policy of WHOIS data.
- This includes **all current registration information available, public and non-public, personal and non-personal**, including email and phone number of registrant, name and postal address of technical and administrative contacts, and billing details, which should continue to be collected by registries and registrars.

## **2.3. Accreditation system**

- **Accreditation** of Law Enforcement and Public Safety agencies which have a legitimate need to access WHOIS data for the purposes mentioned in 2.1, should be carried out at **national level** instead of being carried out centrally, e.g. at European or global level.
- The accreditation system should **ideally guarantee access for other relevant actors**, based on the specific purposes defined pursuant to point 2.1 for processing, including accessing of WHOIS data, comprising non-public elements. This concerns in particular cybersecurity authorities, private sector companies and academic researchers, consumer protection authorities, or intellectual property right holders.
- States should keep an **updated list of public (and private entities) located in their respective jurisdiction**, which are allowed to access non-public WHOIS data on the basis of relevant domestic legislation. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or

---

<sup>7</sup>As recognised by ICANN's Bylaws (ICANN Bylaws Article One, Section 1.1; Section 1.2 (a) Commitments and Core Values; Registration Directory Services Review, §4.6(e))

otherwise processed and to what extent the personal data are or will be processed. Therefore, the list of the public and private entities should be published in a Register which is made accessible to the public.

- This system could be based on the **certification programme** described by ICANN in relation to the second model of the interim GDPR compliant WHOIS system<sup>8</sup>, provided that programme can accommodate the minimum requirements described in this document. The set of requirements for the issuance of certificates should be clear and transparent.

#### **2.4. Authentication of access**

- Authentication mechanisms should be compatible with the rate of look-ups expected from authorised users.
- Nationally-accredited requestors (with a legitimate need to access non-public WHOIS data based on domestic law) should be provided with the necessary level of access to requested WHOIS data through a **unique set of credentials**.
- Access WHOIS data needs to be maintained regardless of location of storage. This could be achieved in practice through a **centralised federated access system**, e.g. hosted by ICANN.

#### **2.5. Access policy, data location and confidentiality**

- Nationally-accredited entities with a legitimate need to access non-public WHOIS data on the basis of domestic law, **should have permanent access to WHOIS data on a query basis**. Access should not be based on individualised requests justifying the purpose for access, specific data elements sought, nor should it be required to provide a subpoena or any other order from a court or other judicial authority to gain access to non-public WHOIS data.<sup>9</sup>
- There should be sufficient guarantees in place to ensure the implementation of the principle of accountability and purpose limitation. The logging and documentation of the queries and safety of the searches should be made available to the competent oversight authorities for the purposes of verifying the lawfulness of data processing, monitoring and auditing and ensuring proper data integrity and security.
- To ensure confidentiality of the requests, WHOIS data look-ups by nationally-accredited and authenticated actors should be anonymised, possibly through a system of hashes, be logged by them for audit purposes and they should not be limited by the number of lookups or time.

#### **2.6. Accuracy and validity of data**

- As stipulated by the **EU data protection legal framework** and in line with the obligations of contracted parties under their contracts with ICANN, personal data shall be accurate and kept up to date.

---

<sup>8</sup> See p. 7 of <https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf>

<sup>9</sup> Previously covered under section 2.3

- Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (retroactive database data correction with regards to the factual data situation found out during the investigation). To comply with the data quality principle, reasonable steps should be taken to ensure the accuracy of any personal data obtained.

### **2.7. Data Retention and Record of historical WHOIS data**

- In order to ensure the availability of historical WHOIS data, the WHOIS system model should allow access to historical domain data retrospectively. Historical domain and IP ownership information<sup>10</sup> is necessary for the success of investigation by LEA and other parties, and thus an adequate retention policy for historical data should be implemented.
- Such records should also be searchable in such a way as to allow for cross-referencing of information, e.g. where the same data set was used to register several sites.
- In line with the storage limitation principle, data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, or scientific or historical research purposes.

---

<sup>10</sup> For example as offered by Domaintools.

**STRATEGIC GOAL 1 - DEVELOP CYBERCRIME AND DNS ABUSE MITIGATION CAPABILITIES**

Develop capabilities of the ICANN and Law Enforcement communities to prevent and mitigate abuse involving the DNS as a key resource

| No. | Work Topic                                | Description/Expected Outcomes  | Completion | PSWG Topic Lead           | Relevant Stakeholders/Processes/Work Products  |
|-----|---|--|------------|---------------------------|--|
| 1.1 | DNS Abuse Reporting                       | Drive development of effective abuse reporting tools and processes promoting effective policy approaches and proactive industry self-regulation and enabling effective contractual compliance enforcement by ICANN   | Q4 2018    | Iranga Kahangama (US FBI) | <ul style="list-style-type: none"> <li>– ICANN <a href="#">Domain Abuse Activity Reporting Project</a></li> <li>– ICANN <a href="#">Identifier Technology Health Index</a></li> <li>– ICANN <a href="#">gTLD Marketplace Health Index</a></li> <li>– <a href="#">SSAC</a> - Establish collaboration mechanisms</li> <li>– Statistical Analysis of DNS Abuse</li> <li>– GAC DNS Abuse Reporting Principles</li> </ul> |
| 1.2 | DNS Industry Due Diligence and Prevention | Work with DNS Industry stakeholders and ICANN to: develop tools and mechanisms to prevent abuse in gTLDs; and facilitate law enforcement investigations across borders   | 2018/2019  | Iranga Kahangama (US FBI) | <ul style="list-style-type: none"> <li>– ICANN <a href="#">Specification 11 3(b) Advisory</a></li> <li>– ICANN <a href="#">Security Framework for Registries to Respond to Security Threats</a></li> <li>– GNSO <a href="#">New gTLD Subsequent Procedures PDP</a></li> <li>– ICANN <a href="#">Privacy/Proxy Services Accreditation</a></li> </ul>  |
| 1.3 | Consumer Safeguards                       | Assist in the developments of ICANN’s Safeguards to protect the public; contribute to and follow-up on relevant ICANN Reviews, Review recommendations and implementation, and liaise with the the Consumer Safeguards Director, as appropriate, to work together to achieve our mutual goal to safeguard consumers | 2018/2019  | Laureen Kapin (US FTC)    | <ul style="list-style-type: none"> <li>– ICANN <a href="#">CCT Review Team</a> – Implementation of Recommendations</li> <li>– ICANN <a href="#">SSR 2 Review Team</a></li> <li>– GNSO <a href="#">New gTLD Subsequent Procedures PDP</a></li> <li>– ICANN <a href="#">Privacy/Proxy Services Accreditation</a></li> </ul>  |

| No. | Work Topic   | Description/Expected Outcomes  | Completion | PSWG Topic Lead                           | Relevant Stakeholders/Processes/Work Products   |
|-----|--|--|------------|---|---|
| 1.4 | Accountability                                     | Review data available on DNS abuse, particularly data available through ICANN’s ongoing data collection systems such as DAAR, highlight this data for ongoing policy development efforts so that future policy is informed by relevant data; Ensure that provisions from the contracts related to DNS Abuse are applied and enforced, as well as reviewed and improved, where needed | Ongoing    | [TBD]                                     | <ul style="list-style-type: none"> <li>– ICANN <u>Contractual Compliance</u> team and mechanisms</li> <li>– GNSO <u>New gTLD Subsequent Procedures PDP</u></li> <li>– GNSO <u>Next-Generation Registration Directory Services (RDS) PDP</u></li> <li>– Development of best practices (e.g. Spec 11)</li> <li>– Raising awareness within and outside the ICANN Community (incl. cross-community sessions during ICANN meetings)</li> </ul> |
| 1.5 | Preventing Exploitation of DNS to Perpetuate Abuse | Identify how the DNS is used to perpetuate abuse (including but not limited to DDOS, Botnets, and facilitating distribution of illegal materials such as those associated with counterfeit drugs and child sexual abuse). Consider building upon the ICANN Beijing Communiqué safeguards and development of policies for subsequent gTLD rounds; support proactive action.           | Q3 2018    | Cathrin Bauer-Bulst (European Commission) | <ul style="list-style-type: none"> <li>– ICANN <u>Domain Abuse Activity Reporting Project</u></li> <li>– GNSO <u>New gTLD Subsequent Procedures PDP</u></li> <li>– <u>.KID/.KIDS New gTLDs String Contention</u></li> <li>– ICANN <u>Auction Proceeds Cross-Community Working Group</u></li> </ul>  |



**STRATEGIC GOAL 2 - PRESERVE AND IMPROVE DOMAIN REGISTRATION DIRECTORY SERVICES EFFECTIVENESS**

Ensure continued accessibility and improved accuracy of domain registration information that is consistent with applicable privacy regulatory frameworks

| No. | Work Topic  | Description/Expected Outcomes   | Completion | PSWG Topic Lead  | Relevant Stakeholders/Processes/Work Products  |
|-----|---|---|------------|--|--|
| 2.1 | Access to gTLD Registration Data                  | Ensure maintenance of swift and effective access to gTLD Registration data for the legitimate needs of civil and criminal law enforcement (including consumer protection authorities) to protect the public and support the public interest | Q2 2018    | Laureen Kapin (US FTC)   | <ul style="list-style-type: none"> <li>– ICANN <a href="#">Whois Compliance with GDPR</a></li> <li>– ICANN <a href="#">Procedure for Handling Whois Conflict with Privacy Laws</a></li> </ul>  |
| 2.2 | Next Generation Protocols and Policies            | Guide the exploration of protocols and policies through active participation in relevant processes and timely input, including on law enforcement requirements for accessing layered RDS  | 2018/2019  | Gregory Mounier (Europol)  | <ul style="list-style-type: none"> <li>– ICANN <a href="#">RDAP Pilot Program</a></li> <li>– GNSO <a href="#">Next-Generation Registration Directory Services (RDS) PDP</a></li> </ul>   |
| 2.3 | Registration Data Accuracy                        | Continue driving initiatives geared towards increasing the quality of gTLD registration data, including by highlighting and leveraging data quality requirements in data protection legislation   | Q4 2018    | [TBD]  | <ul style="list-style-type: none"> <li>– ICANN <a href="#">WHOIS Accuracy Reporting System (ARS)</a></li> <li>– ICANN WHOIS Accuracy Program Specification and <a href="#">Registrar Across Field Address Validation</a></li> <li>– GNSO <a href="#">Next-Generation Registration Directory Services (RDS) PDP</a></li> <li>– GNSO <a href="#">New gTLD Subsequent Procedures PDP</a></li> <li>– ICANN <a href="#">Privacy/Proxy Services Accreditation</a></li> </ul> |
| 2.4 | Performance of ICANN’s Mission in relation to RDS | Monitor ICANN’s performance of its key bylaw responsibilities with regards to accuracy, access and protection of gTLD registration data   | 2019       | Cathrin Bauer-Bulst (European Commission), Lili Sun (Interpol), Thomas Walden (US DEA) | <ul style="list-style-type: none"> <li>– ICANN <a href="#">RDS Review Team</a></li> </ul>  |

**STRATEGIC GOAL 3 - BUILD EFFECTIVE AND RESILIENT PSWG OPERATIONS**

| No. | Work Topic                              | Description/Expected Outcomes   | Completion | PSWG Topic Lead                           | Relevant Stakeholders/Processes/Work Products   |
|-----|---|---|------------|---|---|
| 3.1 | Define Strategy and Workplan            | Define Strategy and Workplan in alignment with PSWG Terms of Reference, GAC guidance and priorities, and ICANN Bylaws, taking into account current challenges and opportunities   | Q1 2018    | Cathrin Bauer-Bulst (European Commission) | <ul style="list-style-type: none"> <li>– PSWG <u>Terms of Reference</u></li> <li>– PSWG Strategy and Workplan</li> <li>– Relevant GAC Advice and Principles</li> <li>– New ICANN Bylaws</li> </ul>  |
| 3.2 | Strengthen Leadership                   | Establish a strong and resilient leadership structure to ensure sustained and coherent PSWG activities  | Q2 2018    | Cathrin Bauer-Bulst (European Commission) | <ul style="list-style-type: none"> <li>– Endorse Co-chair selection criteria</li> <li>– Select New Co-chair</li> <li>– Workload distribution among Topics Leads</li> <li>– Invite new Topic Leads</li> </ul>  |
| 3.3 | Strengthen Membership                   | Provide regular and predictable structure of meetings to address the needs of various GAC and PSWG Stakeholders interested in PSWG activities; ensure outreach to stakeholders unable to (regularly) attend ICANN face-to-face meetings; identify opportunities for contribution to the work of the group in supporting the GAC | Q2 2018    | [TBD]                                     | <ul style="list-style-type: none"> <li>– Weekly leadership meetings</li> <li>– Monthly working group meetings</li> <li>– Intersessional face-to-face meetings</li> <li>– Ad hoc topical meetings and webinars for PSWG and GAC Members</li> <li>– Outreach activities – Newsletter</li> </ul> |
| 3.4 | Reporting and Coordination with the GAC | Ensure alignment of PSWG focus and activities with GAC priorities and GAC consensus decision making, by providing regular opportunities for GAC/PSWG leadership coordination and ensuring GAC review and possible endorsement of key PSWG work products   | Continuous | [TBD]                                     | <ul style="list-style-type: none"> <li>– PSWG Activity Report to the GAC</li> <li>– GAC briefings and webinars</li> <li>– GAC endorsement procedure</li> <li>– Establish effective liaison with GAC Leadership</li> </ul>   |

**STRATEGIC GOAL 4 - DEVELOP PARTICIPATION IN PSWG WORK AND ENSURE STAKEHOLDER INPUT**

| No. | Work Topic   | Description/Expected Outcomes  | Completion | PSWG Topic Lead | Relevant Stakeholders/Processes/Work Products   |
|-----|--|--|------------|-----------------|---|
| 4.1 | Continually Assess Operational Needs and Seek Expert Input | Identify current and future policy issues and opportunities in support of the operational needs of public safety agencies. Seek expert input from public safety agencies, through PSWG Members and relevant international organization and forums, to inform contributions to the GAC and relevant ICANN processes | Continuous | [TBD]           | <ul style="list-style-type: none"> <li>– Input from GAC</li> <li>– Input from PSWG members</li> <li>– Outreach of PSWG members in their agencies, governments and regions</li> <li>– Dedicated meetings, webinars and/or conference calls on key topics</li> </ul>  |
| 4.2 | Develop Awareness of PSWG by Government Agencies           | Communicate regularly on PSWG activities and achievements that are relevant to national government's priorities in order to secure commitment for effective PSWG membership participation  | 2019       | [TBD]           | <ul style="list-style-type: none"> <li>– PSWG quarterly newsletter</li> <li>– GAC capacityBuilding workshops</li> <li>– PSWG monthly calls</li> <li>– Outreach of PSWG members within their agencies, governments and regions</li> </ul>  |
| 4.3 | Lowering barriers to Participation                         | Provide opportunities for effective participation for GAC and PSWG Members, at varying levels of expertise, into PSWG work initiatives   | Q3 2018    | [TBD]           | <ul style="list-style-type: none"> <li>– PSWG Newsletter and regular calls</li> <li>– Leverage GAC website, including access to non-public content for PSWG members</li> <li>– Repository of ongoing PSWG initiatives, briefings and work products</li> <li>– Internal Position Drafting Procedure</li> </ul> |

| No. | Work Topic                 | Description/Expected Outcomes  | Completion | PSWG Topic Lead         | Relevant Stakeholders/Processes/Work Products  |
|-----|----------------------------|--|------------|-------------------------|--|
| 4.4 | Develop Onboarding Program | Create tools, information materials and training opportunities for new participants to ICANN and the PSWG to enable them to quickly become effective in a new environment and contribute with their experience and positions; create mentor/buddy system for new members, especially those attending ICANN meetings for first time | Q2 2018    | Sara Marcolla (Europol) | <ul style="list-style-type: none"> <li>– Updated Law Enforcement Guide to ICANN</li> <li>– Onboarding package</li> <li>– Mentoring System</li> <li>– ICANN Meetings Introduction Program</li> <li>– ICANN introduction presentation at intersessional meeting</li> </ul> |

# GAC PSWG Intersessional Meeting

12 February 2018



Cathrin Bauer-Bulst  
chair

Greg Mounier

Laureen Kapin

Iranga Kahangama

European Commission, PSWG Co-

Europol, PSWG Topic Lead

US FTC, PSWG Topic Lead

US FBI, PSWG Topic Lead

- Introductions
- Housekeeping
  - Agenda
- A quick introduction of the two groups
  - ICANN GAC PSWG
  - EMPACT
- Internet Governance - the special context

- Publicly available database of registration information on each registrant of a domain name.
- Maintained by ICANN and its contracted registries and registrars.

## What information ?

- Domain names details: Domain name, IP address, Name server, creation/expiry date, domain status.
- Information on Registrar
- Registrar's URL, registrar's abuse email, phone number.
- Information on registrants (domain name holder)
- Registrant email, postal address, fax and telephone number.
- Administration contact and technical details

## Address lookup

canonical name [www.vip.icann.org](http://www.vip.icann.org).

aliases [www.icann.org](http://www.icann.org)

addresses **2620:0:2d0:200::7**  
**192.0.32.7**

## Domain Whois record

Queried [whois.publicinterestregistry.net](http://whois.publicinterestregistry.net) with "[icann.org](http://icann.org)"...

```
Domain Name: ICANN.ORG
Registry Domain ID: D2347548-LROR
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2017-12-08T16:40:01Z
Creation Date: 1998-09-14T04:00:00Z
Registry Expiry Date: 2027-12-07T17:04:26Z
Registrar Registration Expiration Date:
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Reseller:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverRenewProhibited https://icann.org/epp#serverRenewProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Registry Registrant ID: C67701347-LROR
```

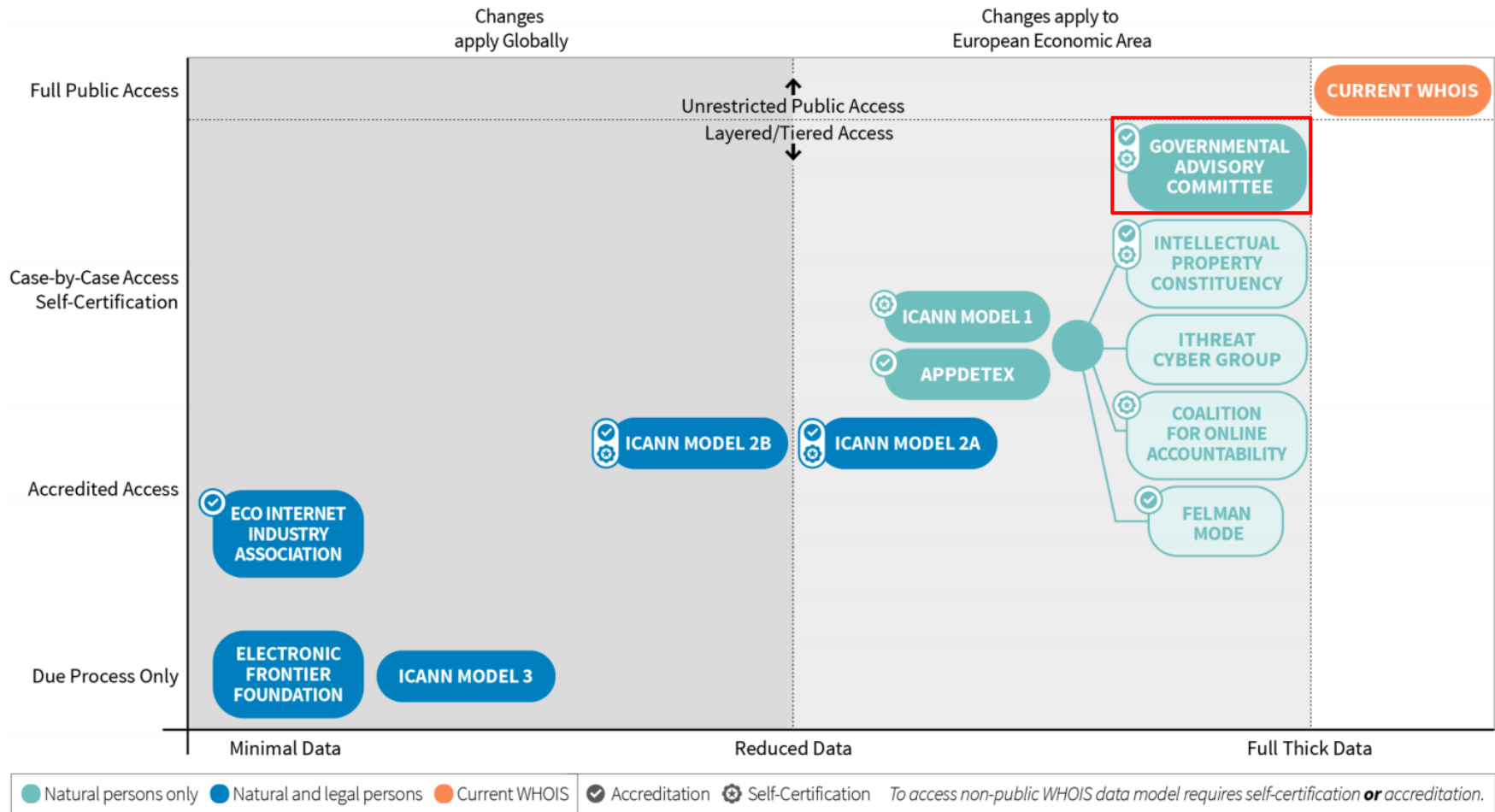


1. Contact point for domain name (notify)
  2. Investigative leads on the owner of a domains
- **Registrant** (name, email, address) = identification, intelligence
  - **Creation Date, renewal:** Recent => DGA? Long time => history check = identification
  - **Registrar** = further inquiry (court order)
  - **Nameserver record** = other domain controlled by registrant
- 
- ★ WHOIS help crime attribution
  - ★ WHOIS is one cyber investigative tool among many others
  - ★ Accurate WHOIS => essential element of online accountability

- Domain registration abuse is at the heart of C2 botnet infrastructure
- New domain names from registrars around the world at fast pace:
  - Sustain takedown requests
  - Sustain sink holing attempts
  - Sustain hijacking attempts
- Banking malware
- **WHOIS lookup** on domain used to administrate botnet => identify a suspect
- WHOIS lookup on the domain => **email address**
- **Reverse WHOIS lookup** => other domains registered with same email
- Domain => Old private website
- Successful arrest and conviction

- Since **2003**: data protection authorities raised concerns about general public availability of all Whois data
- Several **attempts to reform** Whois policy
- Impending entry into force of General Data Protection Regulation has advanced the process
- **November 2017**: announcement of potential suspension of compliance
- **January 2018**:
  - ICANN presentation of 3 possible models
  - Community models submitted in parallel
- In the **next days/weeks**: announcement of chosen model
  - Will likely be applied horizontally across all contracted parties
  - ICANN cannot force contracted parties to violate laws - further exceptions possible

# Proposed Interim GDPR Compliance Models and Selected Community Input (Working Draft)



More on the cited models, including community comments at: <https://go.icann.org/gdprlegal>

Source: ICANN 2 Feb. 2018 Webinar materials and recording, available at: <https://www.icann.org/resources/pages/data-protection-meetings-2017-12-08-en>

- Collection
  - Requirements for Registries and Registrars
  - Public/Non Public Display of data elements
- Access
  - For law enforcement
  - For other parties supporting law enforcement investigation
- Retention
  - Historical records
  - Bulk Access

| Registrant                    | ICANN Model 1  |              | ICANN Model 2<br>Legal and Natural<br>persons | ICANN Model 3                               |
|-------------------------------|----------------|--------------|---|---|
|                               | Natural person | Legal person |   | Legal and natural persons                   |
| Domain Name                   | Display        | Display      | Display                                       | Display                                     |
| Registry Domain ID            | Display        | Display      | Display                                       | Display                                     |
| Registrar WHOIS Server        | Display        | Display      | Display                                       | Display                                     |
| Registrar URL                 | Display        | Display      | Display                                       | Display                                     |
| Updated Date                  | Display        | Display      | Display                                       | Display                                     |
| Creation Date                 | Display        | Display      | Display                                       | Display                                     |
| Registry Expiry Data          | Display        | Display      | Display                                       | Display                                     |
| Registrar Registration        |                |              |   |   |
| Expiration Date               | Display        | Display      | Display                                       | Display                                     |
| Registrar                     | Display        | Display      | Display                                       | Display                                     |
| Registrar IANA ID             | Display        | Display      | Display                                       | Display                                     |
| Registrar Abuse Contact Email | Display        | Display      | Display                                       | Display                                     |
| Registrar Abuse Contact       |                |              |   |   |
| Phone                         | Display        | Display      | Display                                       | Display                                     |
| Reseller                      | Display        | Display      | Display                                       | Display                                     |
| Domain Status                 | Display        | Display      | Display                                       | Display                                     |
| Domain Status                 | Display        | Display      | Display                                       | Display                                     |
| Domain Status                 | Display        | Display      | Display                                       | Display                                     |
| Registry Registrant ID        | Do not display | Display      | Do not display                                | Do not display                              |
| Registrant Name               | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Organization       | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Street             | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Registrant City               | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Registrant State/Province     | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Postal Code        | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Country            | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Phone              | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Phone Ext          | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Fax                | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Fax Ext            | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Email              | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin Name                    | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin Organization            | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin Street                  | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin City                    | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin State/Province          | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin Postal Code             | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin Country                 | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin Phone                   | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Admin Phone Ext               | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Admin Fax                     | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Admin Fax Ext                 | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Admin Email                   | Display        | Display      | Display                                       | Display unless field includes personal data |
| Tech Name                     | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Tech Organization             | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Tech Street                   | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Tech City                     | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Tech State/Province           | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Tech Postal Code              | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Tech Country                  | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Tech Phone                    | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Tech Phone Ext                | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Tech Fax                      | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Tech Fax Ext                  | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Tech Email                    | Display        | Display      | Display                                       | Display unless field includes personal data |
| Name Server                   | Display        | Display      | Display                                       | Display                                     |
| Name Server                   | Display        | Display      | Display                                       | Display                                     |
| DNSSEC                        | Display        | Display      | Display                                       | Display                                     |
| DNSSEC                        | Display        | Display      | Display                                       | Display                                     |

|   | Interim GDPR Compliance Models  |  |   |   |
|---|---|--|---|---|
|   | Model 1   | Model 2  |   | Model 3   |
|   |   | Model 2A   | Model 2B  |   |
| <b>Collection from Registrant to Registrar</b>  | Full Thick Data   |  |   |   |
| <b>Data Transfer from Registrar to Registry</b> | Full transfer of Thick Data   |  |   |   |
| <b>Data Transfer to Escrow Agents</b>           | Full transfer of existing registration data   |  |   |   |
| <b>Public WHOIS</b>                             | Display all current Thick Data, except do not display: (1) email and phone number of registrant, and (2) name and postal address of tech and admin contacts   | Display only Thin Data + email address for Admin and Tech contacts (do not publish the name or any other data about any registrant)  | Display only Thin Data + email address for Tech and Admin contacts (do not publish the name or any other data about any registrant)   | Do not display any personal data in any registration  |
| <b>Access to Non-Public WHOIS Data</b>          | Self-certification – any 3 <sup>rd</sup> party requestor would identify the specific purpose/need for accessing non-public WHOIS data and self-certify that access is necessary for the purposes of the legitimate interests pursued by the requestor. Upon approval by the registry or registrar, the requestor would agree/certify that it would only use data for the limited purpose approved. (Note: the approval process could be likened to the process for registries to approve access to 3 <sup>rd</sup> parties for zone file data.) Registries and registrars may provide additional access as long as it complies with the GDPR and other applicable laws. | Formal accreditation – Establish a certification program for certain user groups, such as law enforcement agencies and intellectual property lawyers, and registries and registrars must provide “certified” requestors access to non-public Whois data based on pre-defined criteria and limitations. The user groups eligible for the certification program and the process for providing access to be developed in consultation with the GAC so that public policy considerations are taken into account. Registries and registrars may provide additional access as long as it complies with the GDPR and other applicable laws. | Formal accreditation as described in Model 2A.  | Legal due process – third parties would be required to provide a subpoena or any other order from a court or other judicial tribunal of competent jurisdiction to gain access to non-public WHOIS data. |
| <b>Scope/Applicability of Model</b>             | Applies to personal data included in registrations of natural persons where registrant, registry, registrar or processing activities are carried out in the European Economic Area.   | Applies to registrations without regard to whether the registrant is a natural or legal person, where the registrant, registry, registrar or a processor are located in the European Economic Area.  | Applies to all registrations on a global basis without regard to location of registry, registrar, registrant, and processing activities, and without regard to type of registrant. (Note: this option provides a blanket interim solution to provide a single, consistent approach across the board.) | Applies to all registrations on a global basis as described in Model 2B.  |
| <b>Data Retention</b>                           | Life of registration + 2 years  | Life of registration + 1 year  | Life of registration + 1 year   | Life of registration + 60 days  |

Source: ICANN Proposed Interim Models (12 Jan. 2018), available at: <https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf>

| Registrant                    | ICANN Model 1  |              | ICANN Model 2<br>Legal and Natural<br>persons | ICANN Model 3                               |
|-------------------------------|----------------|--------------|---|---|
|                               | Natural person | Legal person |   | Legal and natural persons                   |
| Domain Name                   | Display        | Display      | Display                                       | Display                                     |
| Registry Domain ID            | Display        | Display      | Display                                       | Display                                     |
| Registrar WHOIS Server        | Display        | Display      | Display                                       | Display                                     |
| Registrar URL                 | Display        | Display      | Display                                       | Display                                     |
| Updated Date                  | Display        | Display      | Display                                       | Display                                     |
| Creation Date                 | Display        | Display      | Display                                       | Display                                     |
| Registry Expiry Data          | Display        | Display      | Display                                       | Display                                     |
| Registrar Registration        |                |              |   |   |
| Expiration Date               | Display        | Display      | Display                                       | Display                                     |
| Registrar                     | Display        | Display      | Display                                       | Display                                     |
| Registrar IANA ID             | Display        | Display      | Display                                       | Display                                     |
| Registrar Abuse Contact Email | Display        | Display      | Display                                       | Display                                     |
| Registrar Abuse Contact       |                |              |   |   |
| Phone                         | Display        | Display      | Display                                       | Display                                     |
| Reseller                      | Display        | Display      | Display                                       | Display                                     |
| Domain Status                 | Display        | Display      | Display                                       | Display                                     |
| Domain Status                 | Display        | Display      | Display                                       | Display                                     |
| Domain Status                 | Display        | Display      | Display                                       | Display                                     |
| Registry Registrant ID        | Do not display | Display      | Do not display                                | Do not display                              |
| Registrant Name               | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Organization       | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Street             | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Registrant City               | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Registrant State/Province     | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Postal Code        | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Country            | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Phone              | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Phone Ext          | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Fax                | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Fax Ext            | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Registrant Email              | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin Name                    | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin Organization            | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin Street                  | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin City                    | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin State/Province          | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin Postal Code             | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin Country                 | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Admin Phone                   | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Admin Phone Ext               | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Admin Fax                     | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Admin Fax Ext                 | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Admin Email                   | Display        | Display      | Display                                       | Display unless field includes personal data |
| Tech Name                     | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Tech Organization             | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Tech Street                   | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Tech City                     | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Tech State/Province           | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Tech Postal Code              | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Tech Country                  | Do not display | Display      | Do not display                                | Display unless field includes personal data |
| Tech Phone                    | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Tech Phone Ext                | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Tech Fax                      | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Tech Fax Ext                  | Display        | Display      | Do not display                                | Display unless field includes personal data |
| Tech Email                    | Display        | Display      | Display                                       | Display unless field includes personal data |
| Name Server                   | Display        | Display      | Display                                       | Display                                     |
| Name Server                   | Display        | Display      | Display                                       | Display                                     |
| DNSSEC                        | Display        | Display      | Display                                       | Display                                     |
| DNSSEC                        | Display        | Display      | Display                                       | Display                                     |

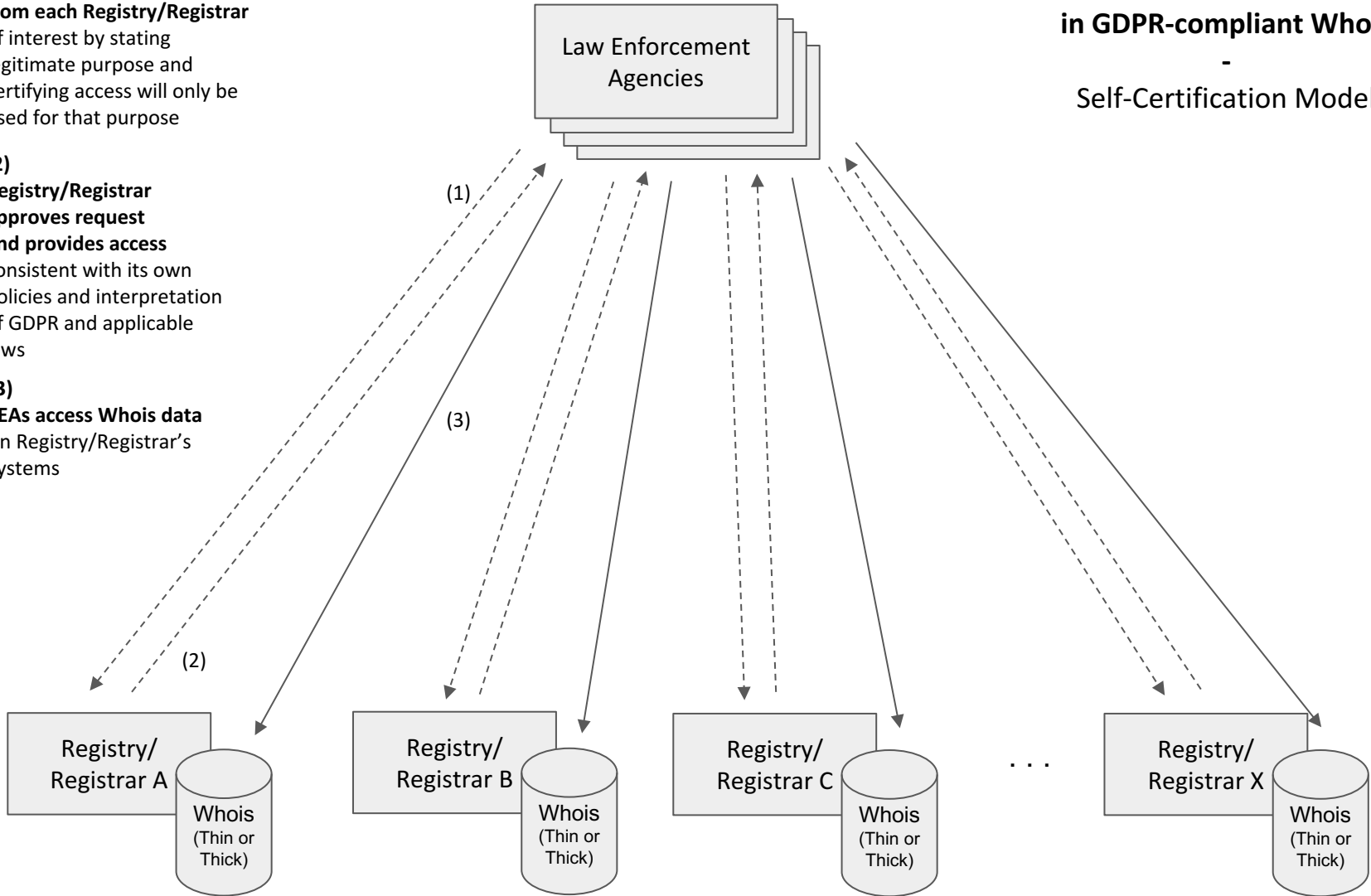
| Registrant                    | Model 4 (GAC/PSWG Proposal) |              |   |
|-------------------------------|-----------------------------|--------------|---|
|                               | Natural person              | Legal person | natural persons                             |
| Domain Name                   | Display                     | Display      |   |
| Registry Domain ID            | Display                     | Display      |   |
| Registrar WHOIS Server        | Display                     | Display      |   |
| Registrar URL                 | Display                     | Display      |   |
| Updated Date                  | Display                     | Display      |   |
| Creation Date                 | Display                     | Display      |   |
| Registry Expiry Data          | Display                     | Display      |   |
| Registrar Registration        |                             |              |   |
| Expiration Date               | Display                     | Display      |   |
| Registrar                     | Display                     | Display      |   |
| Registrar IANA ID             | Display                     | Display      |   |
| Registrar Abuse Contact Email | Display                     | Display      |   |
| Registrar Abuse Contact       |                             |              |   |
| Phone                         | Display                     | Display      |   |
| Reseller                      | Display                     | Display      |   |
| Domain Status                 | Display                     | Display      |   |
| Domain Status                 | Display                     | Display      |   |
| Domain Status                 | Display                     | Display      |   |
| Registry Registrant ID        | Do not display              | Display      |   |
| Registrant Name               | Display                     | Display      |   |
| Registrant Organization       | Display                     | Display      |   |
| Registrant Street             | Display                     | Display      |   |
| Registrant City               | Display                     | Display      |   |
| Registrant State/Province     | Display                     | Display      |   |
| Registrant Postal Code        | Display                     | Display      |   |
| Registrant Country            | Display                     | Display      |   |
| Registrant Phone              |                             | Display      | Display unless field includes personal data |
| Registrant Phone Ext          |                             | Display      | Display unless field includes personal data |
| Registrant Fax                |                             | Display      | Display unless field includes personal data |
| Registrant Fax Ext            |                             | Display      | Display unless field includes personal data |
| Registrant Email              | Display                     | Display      |   |
| Admin Name                    |                             | Display      | Display unless field includes personal data |
| Admin Organization            |                             | Display      | Display unless field includes personal data |
| Admin Street                  |                             | Display      | Display unless field includes personal data |
| Admin City                    |                             | Display      | Display unless field includes personal data |
| Admin State/Province          |                             | Display      | Display unless field includes personal data |
| Admin Postal Code             |                             | Display      | Display unless field includes personal data |
| Admin Country                 |                             | Display      | Display unless field includes personal data |
| Admin Phone                   | Display                     | Display      |   |
| Admin Phone Ext               | Display                     | Display      |   |
| Admin Fax                     | Display                     | Display      |   |
| Admin Fax Ext                 | Display                     | Display      |   |
| Admin Email                   | Display                     | Display      |   |
| Tech Name                     |                             | Display      | Display unless field includes personal data |
| Tech Organization             |                             | Display      | Display unless field includes personal data |
| Tech Street                   |                             | Display      | Display unless field includes personal data |
| Tech City                     |                             | Display      | Display unless field includes personal data |
| Tech State/Province           |                             | Display      | Display unless field includes personal data |
| Tech Postal Code              |                             | Display      | Display unless field includes personal data |
| Tech Country                  |                             | Display      | Display unless field includes personal data |
| Tech Phone                    | Display                     | Display      |   |
| Tech Phone Ext                | Display                     | Display      |   |
| Tech Fax                      | Display                     | Display      |   |
| Tech Fax Ext                  | Display                     | Display      |   |
| Tech Email                    | Display                     | Display      |   |
| Name Server                   | Display                     | Display      |   |
| Name Server                   | Display                     | Display      |   |
| DNSSEC                        | Display                     | Display      |   |
| DNSSEC                        | Display                     | Display      |   |

**MODEL 1 Option 1:  
Access to Non-Public Data  
in GDPR-compliant Whois  
-  
Self-Certification Model**

**(1)**  
Each LEA requests access  
from each Registry/Registrar  
of interest by stating  
legitimate purpose and  
certifying access will only be  
used for that purpose

**(2)**  
Registry/Registrar  
approves request  
and provides access  
consistent with its own  
Policies and interpretation  
of GDPR and applicable  
laws

**(3)**  
LEAs access Whois data  
on Registry/Registrar's  
systems



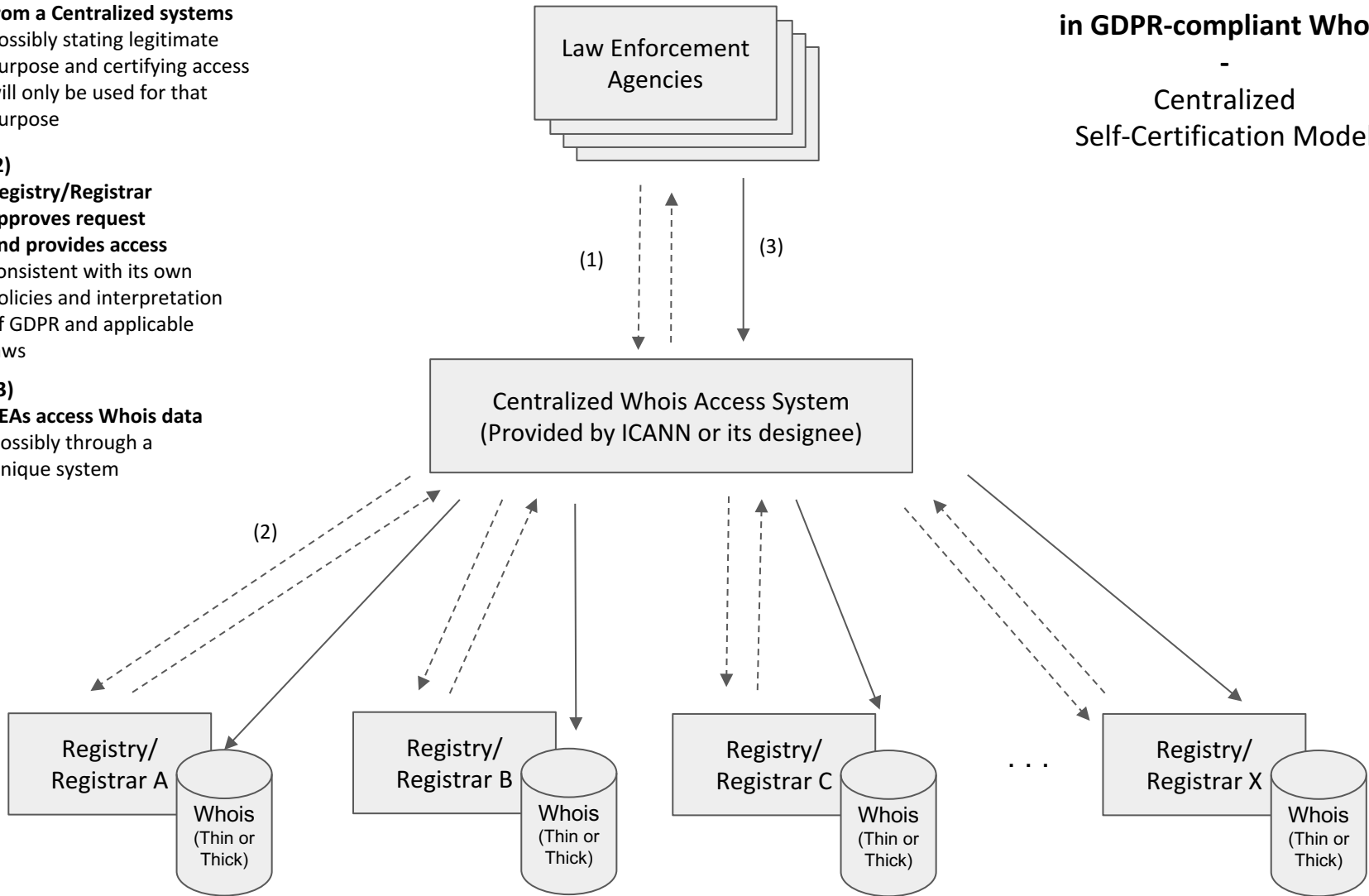


**(1)**  
Each LEA requests access from a Centralized systems possibly stating legitimate purpose and certifying access will only be used for that purpose

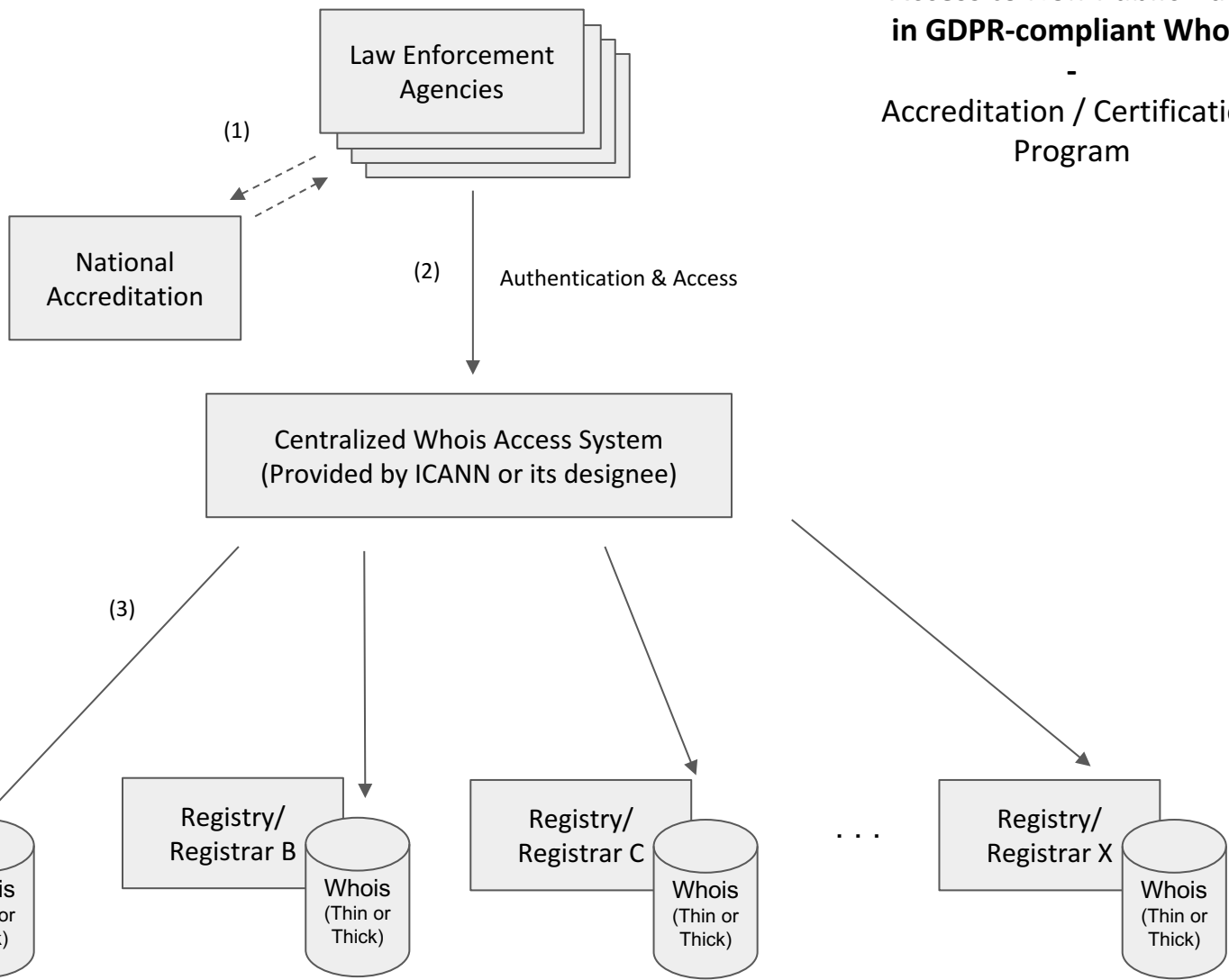
**(2)**  
Registry/Registrar approves request and provides access consistent with its own Policies and interpretation of GDPR and applicable laws

**(3)**  
LEAs access Whois data possibly through a unique system

**MODEL 1 Option 2:  
Access to Non-Public Data  
in GDPR-compliant Whois**  
-  
Centralized  
Self-Certification Model



- (1) LEA accredited through a nationally administered process
- (2) LEA authenticates with a centralized system and access non-public whois data consistent with policies applying across the industry
- (3) LEAs access Whois data possibly through a unique system



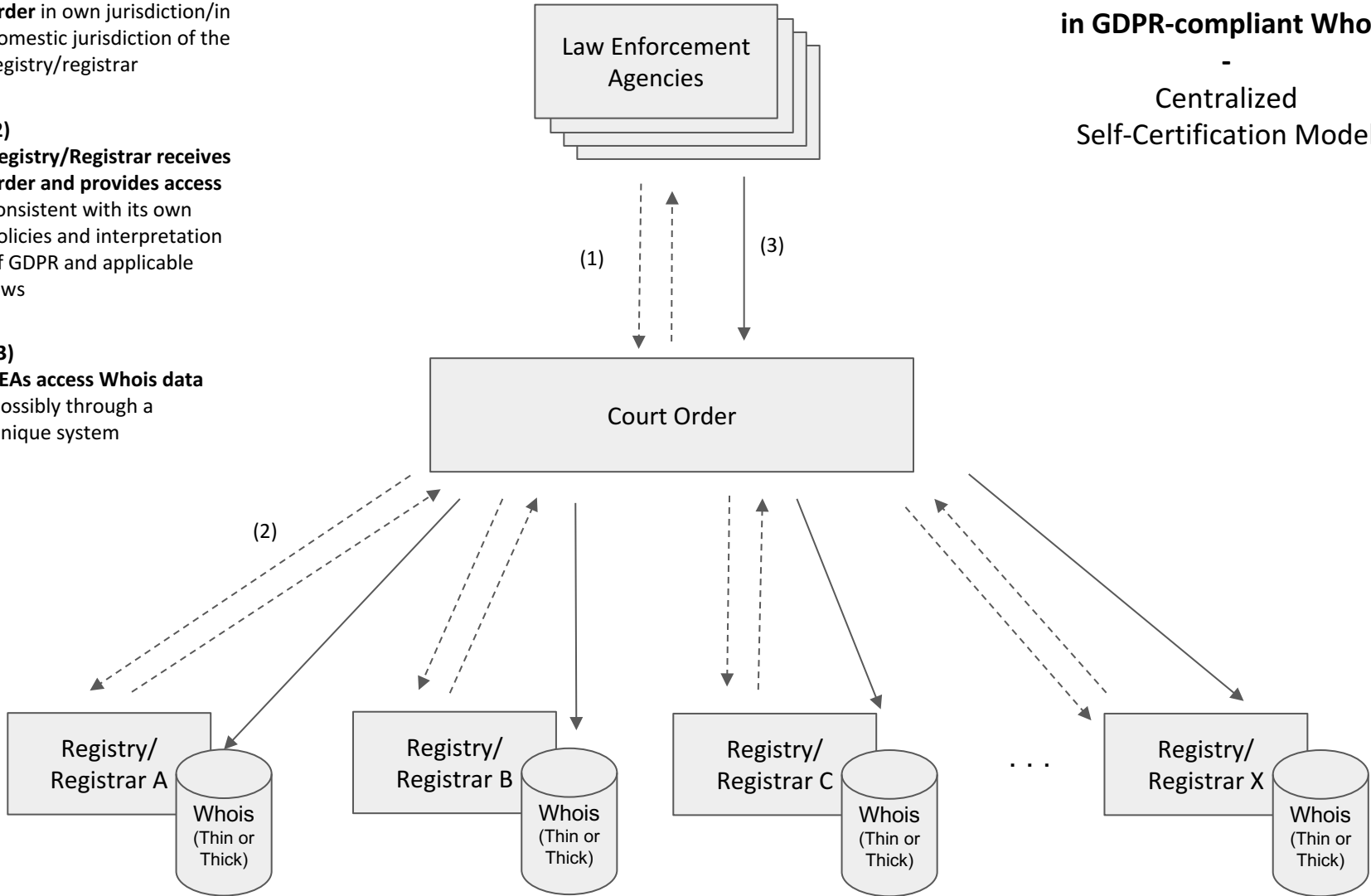
**MODEL 2:**  
**Access to Non-Public Data**  
**in GDPR-compliant Whois**  
 -  
 Accreditation / Certification  
 Program

(1)  
**LEA obtains national court order** in own jurisdiction/in domestic jurisdiction of the registry/registrar

(2)  
**Registry/Registrar receives order and provides access** consistent with its own Policies and interpretation of GDPR and applicable laws

(3)  
**LEAs access Whois data** possibly through a unique system

**MODEL 3:**  
**Access to Non-Public Data**  
**in GDPR-compliant Whois**  
-  
Centralized  
Self-Certification Model



- How many Whois lookups do you make per month? How many lookups does your unit or other units or agencies make?
- Do you use bulk lookup (Port 43), e.g. to download large amounts of Whois data?
- Do you rely on external services provided by private companies in relation to Whois, e.g. DomainTools or others?
- Do you use cross-referencing of Whois data fields, e.g. to identify other domains that were registered using the same information? How often is this used?
- Which data fields are important for your investigations?
- Do you have experience using gated access systems, e.g. on the basis of credentials assigned to you personally or to your organisation? Which requirements exist for your organisation?

## 1. Accreditation system:

- Accreditation of LE and Public Safety agencies with a legitimate need to access non-public WHOIS data should be carried out at **national level**.
- Nationally-accredited actors should have **access to all the WHOIS data necessary** for the fulfilment of their task.
- **Guarantee access for other relevant actors:** CSIRTs, cybersecurity companies, academic researchers, consumer protection authorities, IP right holders.
- States = **updated list of public and private entities** located in their jurisdiction which are allowed to access non-public WHOIS data (**public register**).
- Set of **requirements for issuance of accreditation/certificate** should be clear, transparent and set at ICANN level.

## 2. Authentication and access policy:

- **Centralised federated access system** = provide access based on the list of nationally-authenticated requestors maintained by States.
- Accreditation should be **valid for all registries**.
- Nationally-accredited requestors = access through **unique set of credentials**. (one per agency? One per State?)
- No limit on number of queries + single and bulk access
- Web interface and use of command lines of scripts

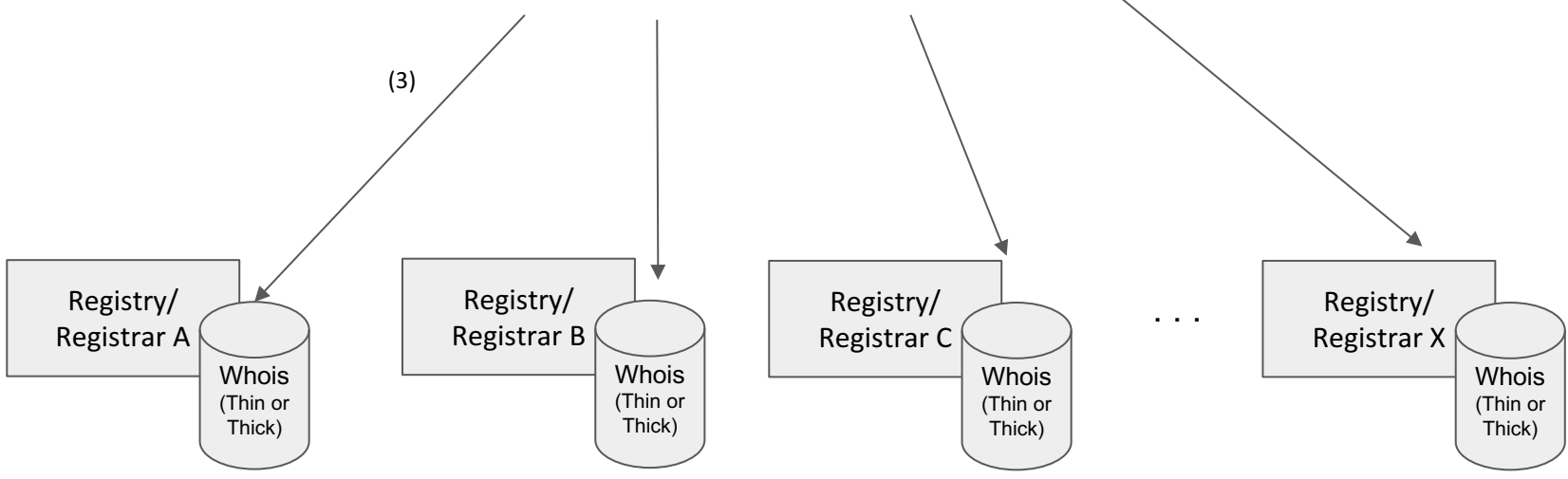
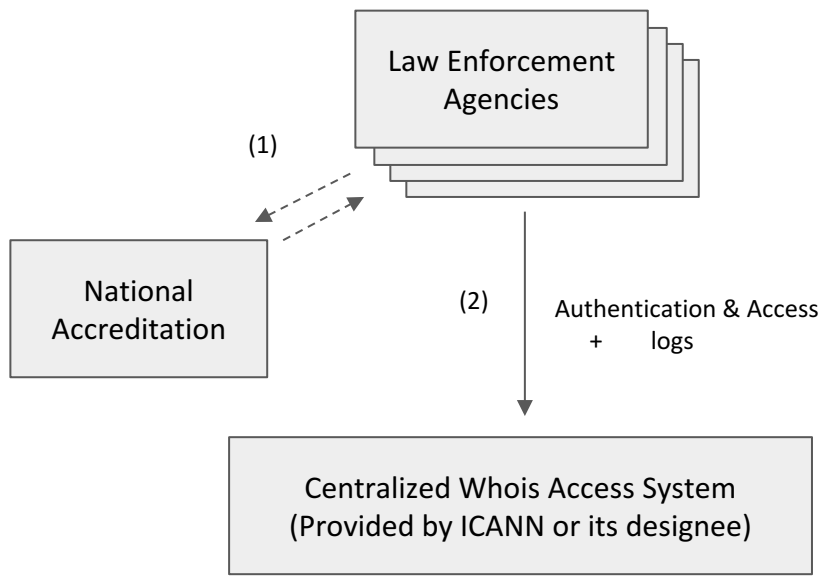
## 3. Confidentiality:

- Queries = **anonymised at central level** (ensure confidentiality of requests + protect investigation)
- **Logging** of queries = at national level + Logs = available to **national competent oversight authorities.**

## 4. Data retention and historical WHOIS data

- Ensure availability of **historical WHOIS**
- What is **adequate data retention policy**? (no longer than necessary).
- Registries/registrars to keep the records? Where is WHOIS data physically stored?
- Can LEA copy the WHOIS database at regular interval?

- (1) **LEA become accredited** through a nationally administered process
- (2) **LEA authenticates with a centralized system and access non-public whois data** consistent with policies applying across the industry
- (3) **LEAs access Whois data** possibly through a unique system



Confidentiality of the queries?

## Access to Non-Public Data in GDPR-compliant Whois - Accreditation / Certification Program



- How to ensure confidentiality of access (logging of requests) ?
- What Audit Trail (Data Protection Accountability Requirement) ?
- Remedy against abuse of LEA access ?
  - Complaint-based system ?
  - Revocation Mechanism

# Widespread Abuse is not Inevitable

- Abuse is neither universal nor wholly random

Registration restrictions: Stricter registration policies correlated with lower levels of abuse

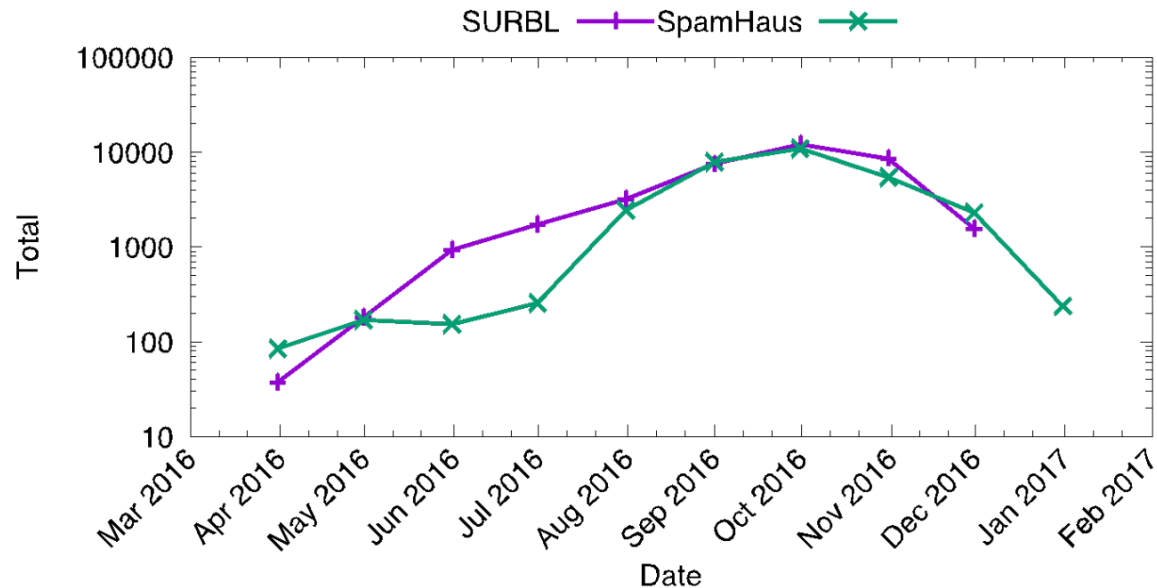
Price matters: operators associated with the highest rates of abuse offered low price domain name registrations

Trademarks as bait: Maliciously registered domain names often contained strings related to trademarked terms

Source:

Secure Domain Foundation, presentation during ICANN60 PSWG Cross Community Session on Abuse Reporting for Fact-Based Policy Making and Effective Mitigation

# The Data Shows a Policy Gap

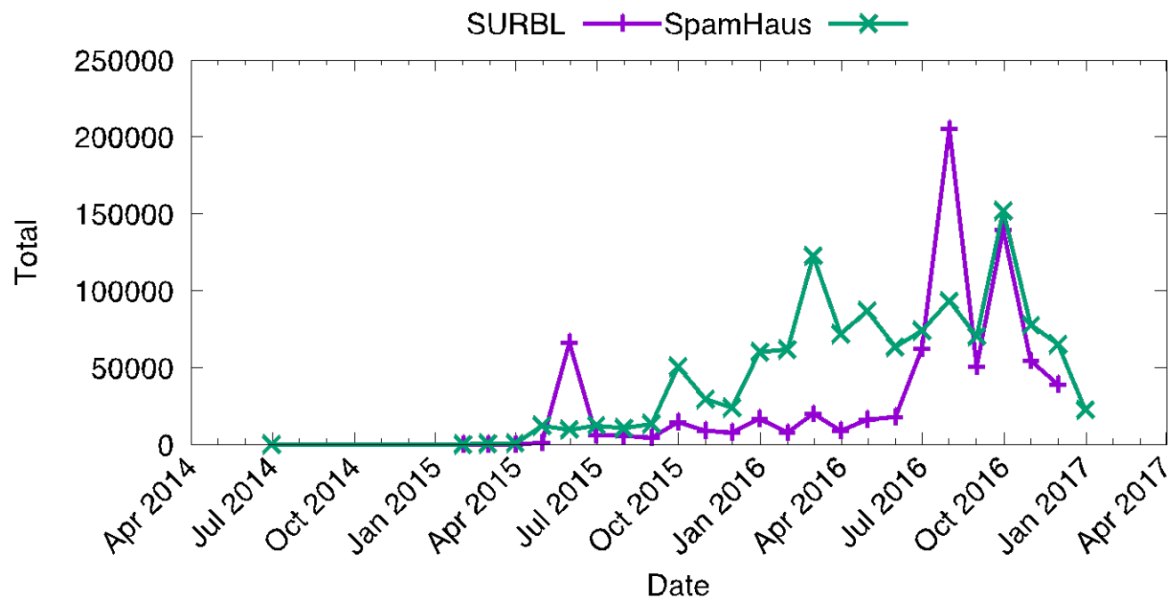


## Nanjing Imperiosus Technology (China)

- More than 93% of the new gTLD registrations sold by Nanjing appeared on SURBL's blacklists.
- ICANN eventually suspended Nanjing in January 2017, citing its failure to comply with the Whois verification, abuse reporting, and record keeping requirements of the RAA and failure to pay ICANN fees.
- However, the sustained, unabated, high abuse rates alone did not constitute grounds for suspension.

Source: Secure Domain Foundation, presentation during ICANN60 PSWG Cross Community Session on Abuse Reporting for Fact-Based Policy Making and Effective Mitigation

# The Data Shows a Policy Gap



## Alpnames Ltd. (Gibraltar)

- Associated with a high volume of abuse from .SCIENCE and .TOP domain names.
- Used price promotions that offered domain name registrations for \$1 USD or sometimes even free.
- Permitted registrants to randomly generate and register 2,000 domain names in 27 new gTLDs in a single registration process.
- Bulk domain names using domain generation algorithms are commonly associated with cybercrime.
- Alpnames remains ICANN-accredited.

Source: Secure Domain Foundation, presentation during ICANN60 PSWG Cross Community Session on Abuse Reporting for Fact-Based Policy Making and Effective Mitigation

1. How do we identify DNS Abuse in a reliable way ?
2. How to create effective and transparent Abuse Reporting ?
3. How could Abuse Reporting support registries and registrars in their prevention and mitigation efforts ?  
How could it be used in contractual compliance enforcement ? How could it be used in policy making ?

# Overview of ICANN and the DNS ecosystem



Jean-Jacques Sahel

PSWG / Europol workshop  
Brussels, 12 February 2018

# Overview

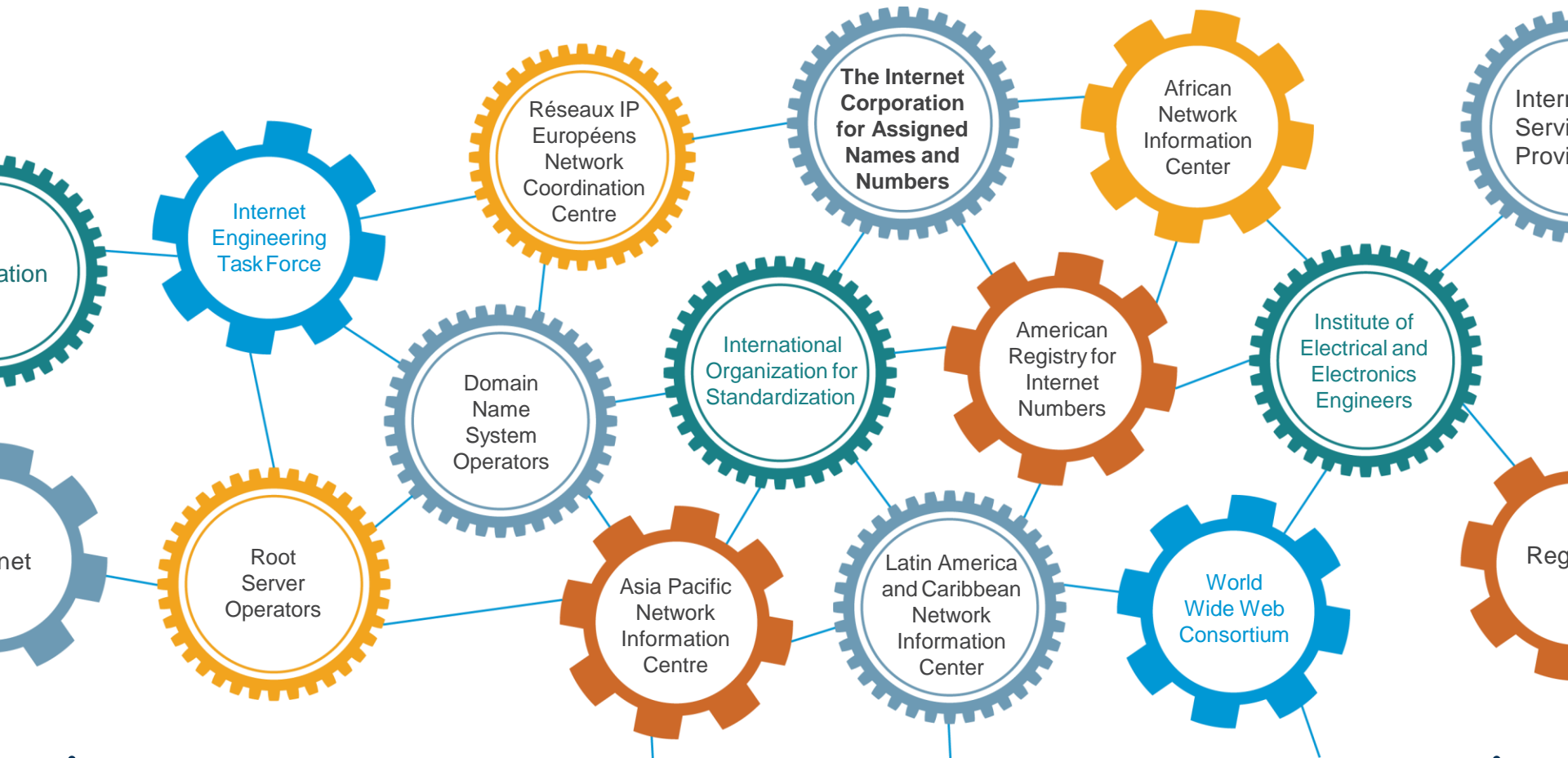
- What is ICANN's role?
- How does it work? ICANN's Multi-stakeholder structure, including the GAC – Governments in ICANN
- Contractual relationship with Registries and Registrars and the Policy development process
- DNS Abuse and awareness - DAAR

# What is ICANN?



# Our Technical Partners

Coordinating with our technical partners,  
we help make the Internet work.



# ICANN's focus: Unique Names and Numbers

Anything connected to the Internet – including computers, mobile phones and other devices – **has a unique number called its IP address.** IP stands for Internet Protocol.



This address is like a postal address. It allows messages, videos and other packets of data to be sent from anywhere on the Internet to the device that has been uniquely identified by its IP address.






IP addresses can be difficult to remember, so instead of numbers, **the Internet's domain name system uses letters, numbers and hyphens, to form a name that is easier to remember.**



# ICANN's Mission

The mission of the Internet Corporation for Assigned Names and Numbers (ICANN) is to **ensure the stable and secure operation of the Internet's unique identifier systems**

Specifically, ICANN:

-  Coordinates the **allocation and assignment of names in the root zone** of the Domain Name System
-  Coordinates the development and implementation of **policies concerning the registration of second-level domain names in generic top-level domains (gTLDs)**
-  Facilitates the coordination of the **operation and evolution of the DNS root name server system**
-  Coordinates the allocation and assignment at the **top-most level of Internet Protocol numbers & Autonomous System numbers**
-  Collaborates with other bodies as appropriate to provide registries needed for the functioning of the Internet as specified by Internet protocol standards development organizations

# Multistakeholder Model and structure

# The ICANN Multistakeholder Community

ICANN follows a bottom-up, multistakeholder model

in which individuals, non-commercial stakeholder groups, industry, and governments

play important roles in its community-based, consensus-driven, policymaking approach.



Learn More ▶

<https://www.icann.org/community>

# The ICANN Community



 [Learn More ▶](#)

<https://www.icann.org/community>

# Supporting Organizations (SOs)



## ASO

The ASO Address Council is composed of 15 volunteers — 3 from each of the Regional Internet Registries (RIRs)— who work on **global Internet Protocol (IP) Address Policy**.



## ccNSO

The ccNSO (Council and members) works on **global policies relating to country code top-level domain name (ccTLD) policies** (e.g., .br, .uk).



## GNSO

The GNSO Council is composed of 21 members — divided into 2 houses (contracted and non-contracted parties) — who work on **generic top-level domain name (gTLD) policies** (e.g., .com, new gTLDs).

## Supporting Organizations (SOs)

Three SOs in the ICANN community are responsible for developing policy recommendations in the areas they represent.

Address Supporting Organization (ASO)

Country Code Names Supporting Organization (ccNSO)

Generic Names Supporting Organization (GNSO)

# Advisory Committees (ACs)

## Advisory Committees (ACs)

Four ACs give advice and make recommendations on ICANN topics.

At-Large Advisory Committee (ALAC)

Governmental Advisory Committee (GAC)

Root Server System Advisory Committee (RSSAC)

Security and Stability Advisory Committee (SSAC)



### ALAC

The ALAC voices the interests of the **individual Internet user** and is composed of 15 members- 2 from each of the five Regional At-Large Organizations (RALOs) and 5 appointed by the ICANN Nominating Committee. It is supported by over 200 At-Large Structures (ALSes) and volunteers.



### GAC

The GAC provides advice on **public policy issues**, particularly on interactions with policies and national laws or international agreements.



### RSSAC

The RSSAC advises the ICANN community and Board on the **operation, administration, security, and integrity of the Internet's Root Server System.**




### SSAC

The SSAC advises on matters related to the **security and integrity of the Internet's naming and address allocation systems.**



# Governmental Advisory Committee (GAC)



**GAC**  
The GAC provides advice on public policy issues, particularly on interactions with policies and national laws or international agreements.

**ICANN | GAC**  
Governmental Advisory Committee



<https://gacweb.icann.org>

Representatives from National Governments

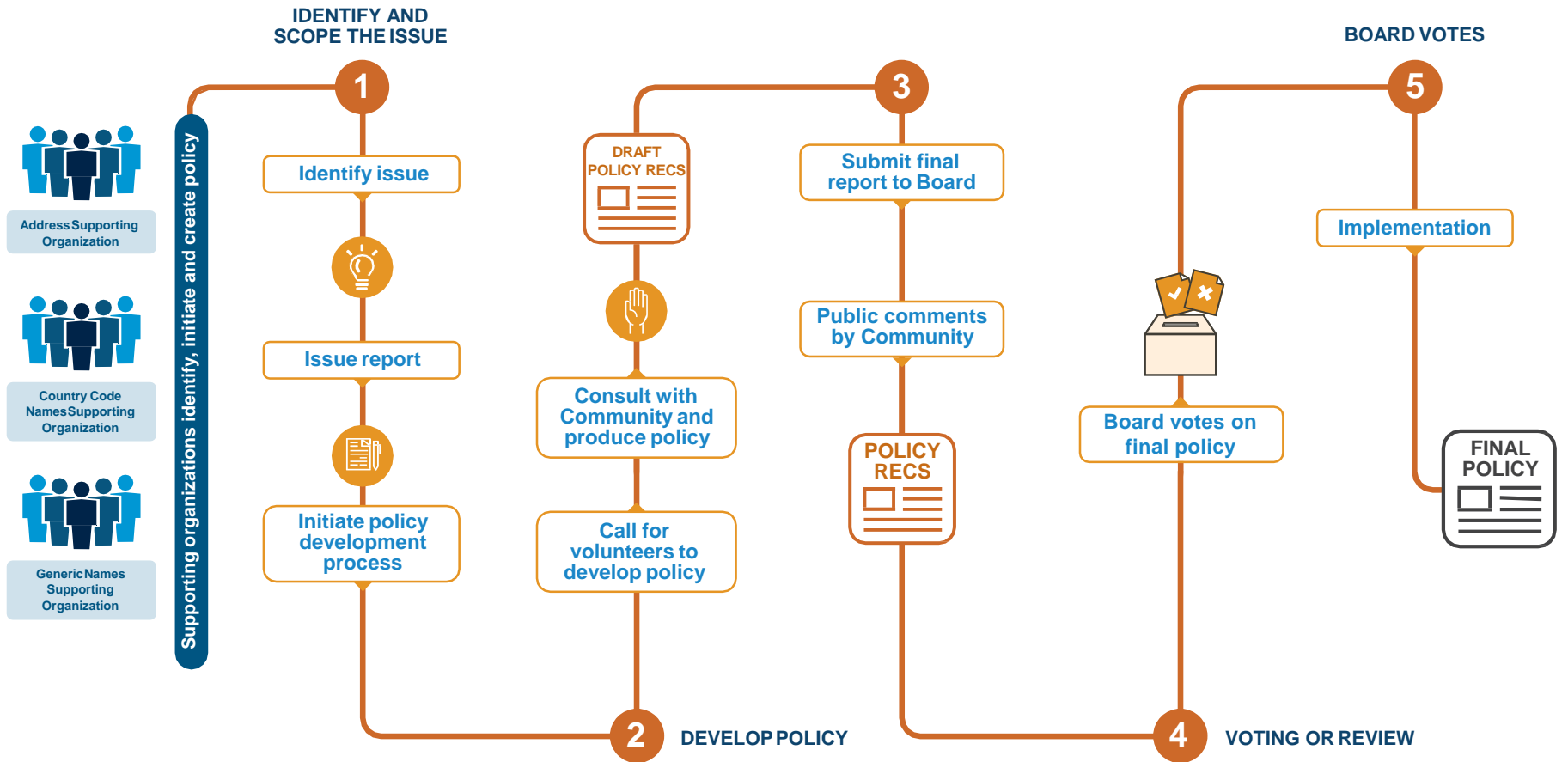
Representatives from Distinct Economies recognized in International Fora

Representatives from Multinational Governmental and Treaty Organizations (usually in observer capacity)

Representatives from Public Authorities (usually in observer capacity)

Public Safety Working Group

# How Does the Community Develop Policy?



Advisory Committees can participate during the process

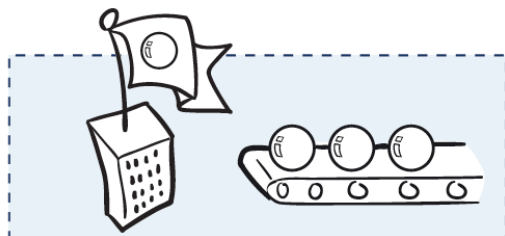
- At-Large Advisory Committee
- Security and Stability Advisory Committee
- Root Server System Advisory Committee
- Government Advisory Committee

# DNS Industry stakeholders and ICANN policy

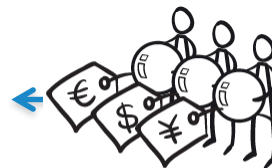
# DNS Industry: Key Stakeholders



ICANN



REGISTRY OPERATOR & SERVICE PROVIDER



REGISTRAR



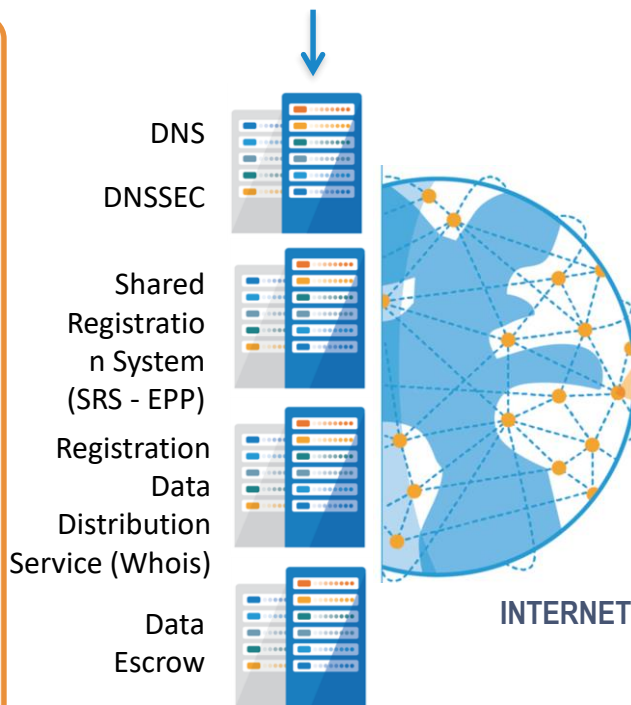
RESELLER



REGISTRANT

## Registries and Registrars

To make sure you get to the correct Internet address, ICANN has contracts with domain name registering companies (Registrars) and organizations responsible for operating Top-Level domains longer than two characters (Registries) around the world



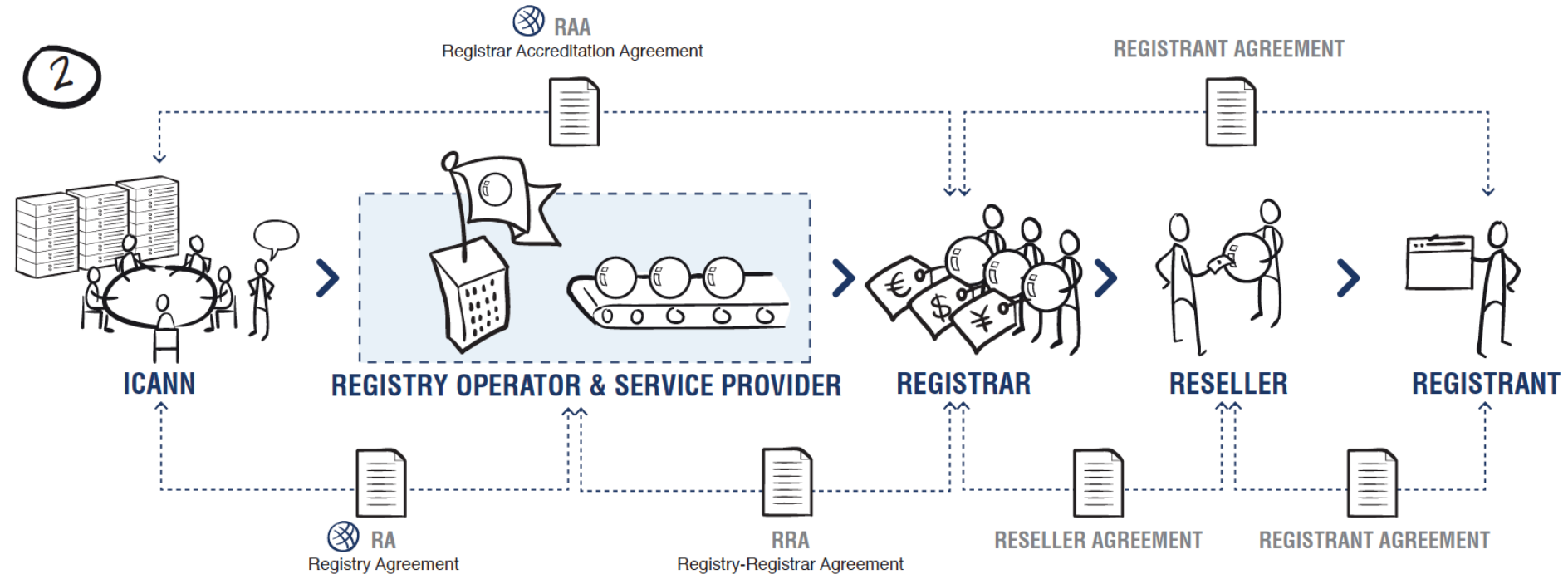
I am the registrant of the "hello" domain name in the .world TLD (Top-Level Domain)



INTERNET USER

I would like to visit the website **www.hello.world**

# DNS Industry and ICANN: Contracts



## Contractual Compliance

- Contracts are enforced through Contractual Compliance.
- The mission is to preserve the security, stability and resiliency of the Domain Name System and to promote consumer trust through prevention, transparency and enforcement

# Cyber-awareness inc. DAAR

# Security (SSR) awareness

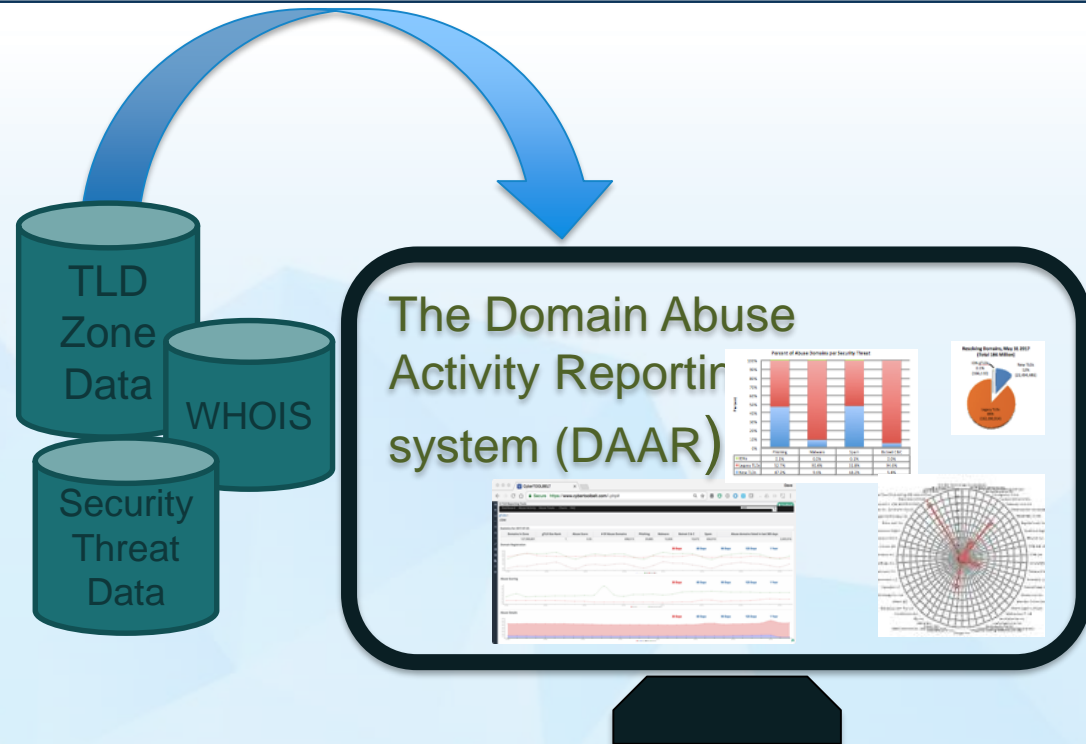
---

Raising user awareness is part of ICANN's overall and security, stability, and resiliency (SSR) remit and includes :

- Data reporting on DNS (Domain name) Abuse
- Data sharing to assist operations or security activities
- Collaboration with the public safety community (e.g., investigations, training)
- Security knowledge transfer

# Data Reporting on Domain Name System (DNS) Abuse

- A system for reporting on domain name registration and abuse data across TLD registries and registrars
- The purpose of this project is to provide ICANN community with data to support consensus policy development

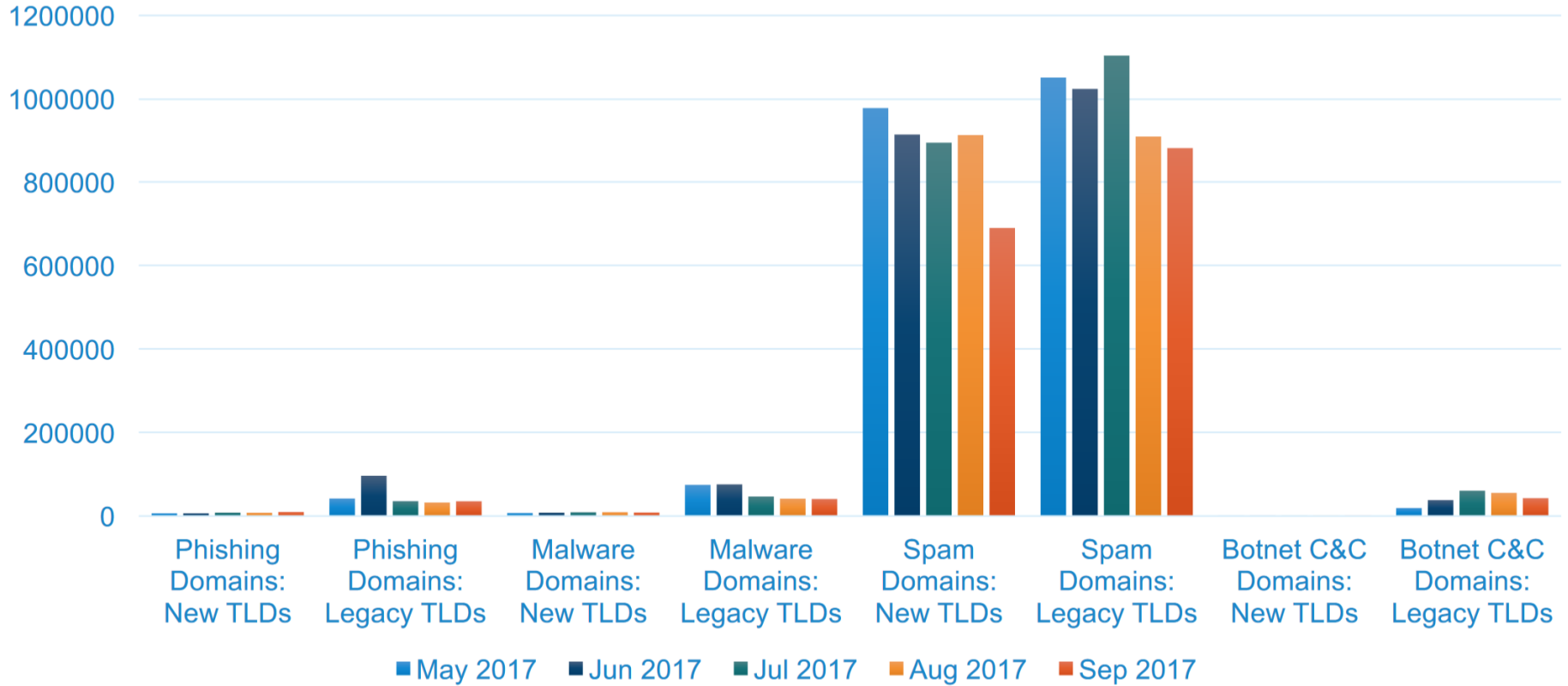


*DAAR reflects how parties external to ICANN community see the domain ecosystem*



# Data Set: All gTLDs having at least 1 reported abuse domain

## Security Threats



# Where is Abuse Concentrated in New TLDs?

| Exploited New TLDs<br><b>MAY 2017</b> | Abuse Domains<br>Reported to DAAR | New TLD Program Resolving<br>Domains for Which DAAR<br>Obtains Data |
|---------------------------------------|-----------------------------------|---|
| 5 most exploited new TLDs             | 56%                               | 22%   |
| 10 most exploited new TLDs            | 73%                               | 34%   |
| 25 most exploited new TLDs            | 97%                               | 70%   |

| Exploited New TLDs<br><b>SEP 2017</b> | Abuse Domains<br>Reported to DAAR | New TLD Program Resolving<br>Domains for Which DAAR<br>Obtains Data |
|---------------------------------------|-----------------------------------|---|
| 5 most exploited new TLDs             | 53%                               | 26%   |
| 10 most exploited new TLDs            | 71%                               | 48%   |
| 25 most exploited new TLDs            | 95%                               | 67%   |

TLDs for which no abuse domains were reported are not included in the counts

Latest report :

<https://www.icann.org/en/system/files/files/presentation-daar-31oct17-en.pdf>

# Next

---

- **ICANN61 Puerto Rico, March 10-15**
- **GDD Summit, Vancouver 14-17 May 2018**



- **ICANN62**



- **ICANN63 in Barcelona, 20 - 26 October: 20th AGM; 4<sup>th</sup> High Level Government Meeting**

# Get Involved and Informed



**Attend an ICANN Public Meeting.** Three times a year, ICANN holds free and open public meetings in different regions around the world. Visit [meetings.icann.org](https://meetings.icann.org) to learn more.



Visit [go.icann.org/journey](https://go.icann.org/journey) to learn how you can attend an ICANN Public Meeting as part of the NextGen@ICANN or ICANN Fellowship programs.



Take a free online course at [learn.icann.org](https://learn.icann.org).



Attend events in your region.



Find and participate in an ICANN community group by visiting [icann.org/community](https://icann.org/community).



Sign up for ICANN news alerts and regional newsletters.

# Thank you and questions



One World, One Internet

Visit us at [icann.org](https://icann.org)



[@icann](https://twitter.com/icann)



[facebook.com/icannorg](https://facebook.com/icannorg)



[youtube.com/icannnews](https://youtube.com/icannnews)



[flickr.com/icann](https://flickr.com/icann)



[linkedin/company/icann](https://linkedin/company/icann)



[slideshare/icannpresentations](https://slideshare/icannpresentations)




[soundcloud/icann](https://soundcloud/icann)

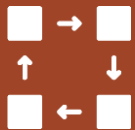
# ANNEXES


# ICANN's Mission

In performing its Mission, ICANN will act in a manner that complies with and reflects ICANN's Commitments and respects ICANN's Core Values

These Commitments and Core Values include:

- 

1 Preserving and enhancing **stability, security, resiliency,** and **openness** of the DNS and the Internet
- 

2 Employing **open, transparent** and **bottom-up,** multistakeholder policy development processes that are led by the private sector
- 

3 Operating with **efficiency** and **excellence,** in a fiscally responsible and accountable manner



Learn more ▶

[www.icann.org](http://www.icann.org)

# Annex - Cyber-awareness



# Data Sharing: Open Data Initiative

---

- ICANN Open Data Initiative
  - Facilitates access to data that ICANN organization or community creates or curates (zone data, protocol registries)
  - Access in machine- and human friendly formats
  - Data *registries* that ICANN curates includes:
    - ▶ Top level domain delegations
    - ▶ Accredited registrar
    - ▶ Internet protocol registries (databases)
- One of the goals: to improve collaboration with operational security communities, participation in ICANN

# Operational Security data sharing

---

- As part of daily operational security activities, ICANN staff
  - Exchange public information with private or public sector investigators to assist in global threat mitigation
  - Facilitate cooperation between domain name ecosystem parties, law enforcement and court systems that are instrumental in executing multi-jurisdictional actions against criminal operations or conspiracies

# Security knowledge transfer

---

- ICANN's Office of the Chief Technology Officer (OCTO) publishes data, research papers, or reports to inform the Internet community about:
  - Evolving cyber-threat landscape
  - Advisories or analyses of incidents affecting the DNS
  - Security Awareness articles
  - Research papers, technical articles in cybersecurity or Internet technology journals