GDPR Compliance / ICANN Interim Model Selection for WHOIS (slot I)

Vicky Sheckler, Recording Industry Association of America (IPC)
Tatiana Tropina, Max Planck Institute for Foreign and International Criminal Law (NCUC)

Non-Contract Party House Intersessional
2 February 2018

ICANN stated goal for Compliance Model

- **GOAL:** “Ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible.”

- **GUIDED BY ICANN’s MISSION STATEMENT:** “Subject to applicable laws, ICANN shall use commercially reasonable efforts to enforce its policies relating to registration directory services and shall work with Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to generic top-level domain registration data, as well as consider safeguards for protecting such data.”

Compliance Models – ICANN – Model 1

- Applies only to personal data of a natural person.
- Applies where Ry/Rr are established in EU, or outside EU but provide services to EU data subjects or process data in EU.
- Ry/Rr must display in public WHOIS: (1) domain name, (2) nameserver(s), (3) registrar, (4) creation date, (5) expiration date, (6) registrant name and postal address, (7) admin contact email address, telephone and fax number, and (8) tech contact email address, telephone number and fax number.
- Ry/Rr retain data for 2 years beyond life of registration.
- Ry/Rr must respond to requests for non-public data on a timely basis.
  - Requestors must submit application stating specific purpose for accessing the data.
  - Requestor would self-certify that requested access is necessary for legitimate interests and use limited to such purpose.

Compliance Models – ICANN – Model 2

- Applies to all personal data regardless of natural or legal person.
- Applies:
  - Where Ry/Rr are established in EU or are outside EU but provide services to EU data subjects or process data in EU (Model 2A), or
  - To all registrations globally without regard to Ry/Rr/Rt location (Model 2B)
- Ry/Rr must display in public WHOIS: (1) domain name, (2) nameserver(s), (3) registrar, (4) creation date, (5) expiration date, (6) admin contact email address, and (8) tech contact email address.
- Ry/Rr retain data for 1 years beyond life of registration.
- Formal accreditation/certification program for access to non-public data based on pre-determined criteria.

Compliance Models – ICANN – Model 3

- Applies to all personal data regardless of natural or legal person.
- Applies to all registrations globally without regard to Ry/Rr/Rt location.
- Ry/Rr must display in public WHOIS: (1) domain name, (2) nameserver(s), (3) registrar, (4) creation date, and (5) expiration date.
- Ry/Rr retain data for 60 days beyond life of registration.
- Ry/Rr only grant data access to third-party requestors when required by applicable law and subject to due process requirements (e.g. subpoena, court order).

Compliance Models - Community

- Community members representing variety of stakeholders developed and submitted proposed compliance models:
  - Eco Model
  - ICANN Redaction Model
  - AppDetex / Expert Working Group (EWG) Model
  - Coalition for Online Accountability (COA) Model
  - iThreat Cyber Group (iThreat) Model
- Summary and comparison of these five models in Appendix.

Recent EC Guidance on GDPR/WHOIS

from letter from EC to Mr. Marby dated January 29, 2018

- Acknowledges the importance of the following “public policy objectives” of use of WHOIS system: “identification of contact points for network operators and administrators, help in countering intellectual property infringements, finding the source of cyber-attacks or assistance to law enforcement investigations” and the “corresponding need to preserve WHOIS functionality and access to its information.”

- Acknowledges that at “the same time, there is a need to comply with the GDPR” noting that this is “important not just to ensure respect for the fundamental right to personal data protection, but also for the stability, robustness and accuracy of the WHOIS system as an integral part of the infrastructure that allows the global interoperability of internet services.”

Recent EC Guidance on GDPR/WHOIS, CONT

- Notes following GDPR data principles relevant to WHOIS:

personal data principle	principle of purpose limitation	principle of lawful processing
data minimization principle	data accuracy principle	principle of limited data retention

- Offers the following points in identifying a solution:
  - Distinction should be made between personal data of natural persons which falls within the GDPR and other data
  - ICANN should clearly specify the different purposes for processing, ensure registrants are aware of this, and the registrars know what data to collect and for what purposes, in keeping with the aim to maintain the WHOIS to the fullest extent possible
  - For data subject to GDPR, ICANN should carefully consider to the extent data may continue to be public or whether some restriction should be introduced to ensure that accessible information is relevant and limited to what is necessary in relation to the different purposes of processing
  - In creating such a system the implementation of safeguards against abuse should be considered to ensure a level of security appropriate to the risk.
  - If a system based on accreditation is considered, then the mechanism for accreditation and subsequent access has to respect and ensure the confidentiality of communication.

Summary of Selected Comments to Interim Models

Commenter	Model Favored (if any)	Summary
Select contracted parties	Support ECO model; criticize all 3 interim models	Model 1 doesn't provide justification for publishing personal data; model 2 lacks workable certification program; model 3 fails to satisfy other stakeholders interested in preserving status quo of WHOIS
RrSG	Presumably support ECO model; criticize all 3 interim models	Refers to eco comments. Eco comments note problems with each of the interim models proposed by ICANN; calls for treating data from legal and natural persons in the same manner; notes limitation of access of whois data for third parties in model 3 is too strict
IPC	Model 1, possibly model 2 with changes	Notes model 1 should only apply to data associated with natural persons; registrant email should be in public record, tiered self certification should work; registrars should be required to provide data; model 3 unacceptable
BC	Model 1, possibly model 2 with changes	Notes model 1 should only apply to data associated with natural persons; registrant email should be in public record, tiered self certification should work
NCSG	Model 3, model 2 might be acceptable under certain conditions	Recommend a centralized accreditation model for access to non-public data, wants legal due process for gaining access to non-public information; notes that under model 3, it may be within ICANN's mission to include email address of technical contact and possibly name of registrant in public record

Commenter	Model Favored (if any)	Summary
GAC	GAC Model (criticizes all interim models)	GAC model requires all fields to be public unless they contain personal data; data should be retained for 2 years; should have an accreditation system for access to personal data that allows all legitimate parties to have access; should use a self-certification system until accreditation system is implemented; should only apply w/in scope of GDPR; includes info on legitimate interests for public access to WHOIS data Model 1 – lack of registrant email problematic; self-accreditation too subjective and ineffective; Model 2 – conflate natural and legal persons; uniform approach to data fields is overreach; 1 year data retention too short; Model 3 – subpoena hinder timely access/unreasonable burden; 60 days data retention too short
USG	n/a	Need thick whois, need all legitimate purposes permitted; as much registrant data as possible should be displayed; distinguish btn natural and legal persons; access to PI withheld by GDPR should not be unduly restricted/burdensome for legitimate access; tiered access ok, 2 year data retention necessary; bulk access to third parties should be available

Questions About Interim Model Approach

From Previous Panel

- Who and how to "settle on" a model?
- Why just a single model?
- Will Registries & Registrars be required to use the model?
- How to adjust to operational experience and legal review as the model is implemented ?
- Do the models respect, reflect and/or take into account the views of internet end users, registrants, contracted parties, govt, private sector, other stakeholders?

Additional Questions

- Does ICANN legal have a preferred approach as this stage?
- How has/will ICANN take into account comments received to date? From GAC/govt? Stakeholders? Others?
- Has ICANN requested guidance from the Article 29 working group? When is that advice expected to be received? Will it be shared?
- What are ICANN's next steps in selecting a model?
- Other participant questions?

Questions re: Next Steps

- After a model/s has been selected, will it be subject to further review by regulatory authorities before / after being published? Will it be put before the EU data protection board?
- How does ICANN plan on rolling out the model/s? Enforcing compliance?
- How does ICANN expect the interim model/s selected to impact / inform the RDS PDP?

Appendix

	iThreat	COA	ECO	Redaction	AppDetex
Public Whois	• Thin data • Thick data for legal persons • PII masked for natural persons	<u>Legal</u> • Non PII is public • Registrant can opt out <u>Natural</u> • Non PII is public • Consent sought for PII • With consent full record is public • Consent must be withdrawable	• Domain name • Registry domain ID • Registrar Whois server • Registrar URL • Updated date • Creation date • Registry expiry date • Registrar IANA ID • Registrar abuse contact • Domain status • Name server • DNSSEC • Name server IP address • Last update of Whois	<u>Legal</u> • Fully public except for PII chosen to be redacted <u>Natural</u> • Can apply for redaction of PII • Contactability maintained by anonymized email addr. Escrow has “true data” at all times.	Minimum data set displayed • Domain • Registrant country • Registrar data • Registry data • Anonymized email <u>Nat. persons not in EU / Registry and registrar not in EU</u> • All data public <u>Legal person</u> • GDPR doesn’t apply • Registrants advised to anonymize PII

	iThreat	COA	ECO	Redaction	AppDetex
Access	No layering or gating	• Gated • Self-certification model • Registrant can object to disclosure	• Layered access for LEAs, IP att'ys, others • Trusted clearinghouse model for arbitration of access	ICANN Org runs credentialing program. Fees for: • TMCH SMD holders • LEAs • Others with "legitimate" interests according to GAC principles	Follows EWG: • Logs all access • Access gated for more sensitive data • Access audited to prevent abuse • ToS binds requestor to GDPR compliant terms

	iThreat	COA	ECO	Redaction	AppDetex
Scope	Regionality not addressed	Applies to: • Processing of personal data in context of activities in establishment of registrar in EU • Processing of personal data of EU data subjects in context of registrars outside EU but offering services in EU	Data handling will be uniform, due to difficulties with differentiation between data.	Applies to identified or identifiable natural person that is subject to GDPR, so it is not intended to apply globally	The model has been created to address the processing of personal data in the context of the activities of a data controller or a data processor within the EU, regardless of whether the actual processing takes place within the EU or not, in compliance with Art. 3 GDPR.