

Link to Org Answers sent to Scoping Team on Wednesday January 12, 2022:

<https://community.icann.org/pages/viewpage.action?pageId=184996761>

Scoping team follow up questions / comments from 13 January 2021 Scoping Team Meeting:

1. How is the Compliance team trained on GDPR specifically?

ICANN Contractual Compliance enforces the Registrar Accreditation Agreement, Registry Agreements and Consensus Policies, and its staff are extensively trained on these agreements and policies. ICANN Contractual Compliance does not enforce laws or regulations which are outside the contractual scope of the ICANN organization. Accordingly, the ICANN Contractual Compliance team does not undergo GDPR specific training (or that of any other law or regulation), but subject-matter experts do maintain a general awareness of GDPR issues relevant to their areas of compliance expertise. Each contracted party must ensure its own processing complies with GDPR, where applicable, as well as any other applicable laws and regulations.

2. Are the metrics from Compliance based on complaints received? (Answer: yes.) Would be interested to know – prior to the GDPR, how did ICANN perform these checks?

As noted in real-time during the discussion, metrics from Compliance are based on complaints received. Prior to the transition to the Naming Services portal (NSp) on 29 August 2020, ICANN did not track complaints received by reporter type, as the level of granularity in reporting was limited within the legacy system. ICANN Contractual Compliance's monthly dashboard contains historical data about complaints received/closed that are related to accuracy which is available [here](#). Additional information specifically addressing complaints received before and after GDPR went into effect is available [here](#).

3. What is the status of the DPA negotiation between ICANN org and contracted parties?

Following the Board's adoption of the EPDP Phase 1 Recommendations, ICANN org and a group of registry and registrar representatives designated by the CPH have been working on a document to implement EPDP Phase 1 Recommendations 19 and 20. At present, we are aiming to produce a draft Data Processing Specification to the Registry Agreement and Registrar Accreditation Agreement, which, once finalized, a contracted party could elect to enter into for purposes of data protection compliance. We have made significant progress toward a draft that will, once tentatively agreed, be shared with the Implementation Review Team (IRT) for feedback. In late 2021, ICANN org and the CPH group held extended discussions regarding remaining open issues with the aim to bring this effort to completion in the near term. We expect that this will be ready to share with the IRT prior to the draft Registration Data Policy document (the product of the EPDP Phase 1 IRT's work) being published for public comment.

4. Is the ability for ICANN to share any of the training materials possible? (For example, it has been difficult for the group with respect to wordsmithing. If there are documents regarding clarity on these issues, it would be very helpful.)

ICANN Contractual Compliance utilizes written training materials, as well as regular in-person and phone/video training sessions conducted by senior staff. These training materials contain information about our systems, internal procedures and processes and are, therefore, confidential. Such materials, however, do not seek to define or interpret contractual requirements, and use the defined terms and requirements within the Registrar Accreditation Agreement, Registry Agreements, and Consensus Policies.

5. With respect to Q3, it discusses issues that are out of scope. How would a third party complainant ever file a complaint regarding the accuracy of registrant data behind a P/P service? When is a complaint in scope and when is it out of scope?

ICANN refers the team to the prior response to question #20. In-scope complaints pertaining to customer data of a P/P Service Provider are limited. For example, if the underlying customer is also the Account Holder, or where the service provides an anonymized email that forwards to the underlying customer email (such that an inaccurate underlying email would result in a bounce-back from the email in the public Registration Data).

ICANN additionally notes that the majority of P/P services are “Proxy Services”, which are “service[s] through which a Registered Name Holder licenses use of a Registered Name to the P/P Customer in order to provide the P/P Customer use of the domain name, and the Registered Name Holder’s [RNH] contact information is displayed in the Registration Data Service (Whois) or equivalent services rather than the P/P Customer’s contact information.” (See Section 1.3 of the Specification of Privacy and Proxy Registrations). In such cases, the “registrant data” is the data of the Proxy Service/RNH.

6. With respect to the engagement you are doing on the NIS2...exactly what kind of purpose are you lobbying for? How does it fit with ICANN’s controller role? Who else do you think should be able to avail themselves of that “legitimate purpose” role to check accuracy? Do you envisage outsourcing and how would that work? Who are you engaging with, the EC or the DPAs?

As regards the ongoing negotiations on NIS2, ICANN org is engaging with the co-legislators, i.e. the European Parliament and the Council of the EU. The purpose of the engagement is to explain how the DNS works, highlight what the community is working on, and identify the challenges the community is facing with respect to the application of GDPR to registration data in the context of the ICANN policy making. This engagement is with the aim to ensure that deliberations and decisions relating to the DNS in NIS2 are made with a full understanding of the current situation and possible impact of the proposed legislation.

With respect to registration data accuracy, ICANN org provided information about the requirements to perform due diligence checks as developed by the ICANN community and applied through contractual

structures with the contracted parties, as well as information about how ICANN compliance enforces these requirements, including how GDPR has affected ICANN compliance's ability to enforce accuracy requirements.

Regarding the question, "How does it fit within ICANN's controller role[?] (emphasis added)", the intended meaning of "it" is unclear. However, as regards the "purpose," if a purpose for registration data processing and recognition of a legitimate interest in processing that data (where the GDPR applies), were codified in a European directive and in turn in implementing member state laws, this could provide helpful clarity for any controller of the processing of personal data within registration data. The question ("Do you envisage outsourcing and how would that work?") is also unclear (what would ICANN be potentially outsourcing?) and, thus, an answer on this aspect of the question cannot be provided.

7. In the answer to Q21, the second to last line uses the term "patently inaccurate". How is "patently inaccurate" determined? For example, the name Mickey is an actual name. There are times where data may look fishy but is, in fact, correct. How does ICANN org make this determination?

ICANN Contractual Compliance takes into account the totality of the information/evidence available. For instance, in the example provided, a fictional address "1234 Main Street, Disneyland, 00000, USA" combined with the Registrant Name "Mickey Mouse", would be sufficient to suggest that the data is incorrect. ICANN Contractual Compliance further notes that it does not independently make determinations of accuracy, but may initiate a notice or inquiry where the information/evidence suggests that such contact information is incorrect.