

Emails to [jennifer.scott@icann.org](mailto:jennifer.scott@icann.org) from Trang Nguyen on 4 October 2018

**1. ICANN Compliance to provide a general overview regarding how data escrow files are used in the course of an audit. Included within the overview, ICANN Compliance should include more information around the potential decryption of data escrow deposits during the course of an audit.**

*In past audits of registry operators, ICANN Contractual Compliance has requested from Data Escrow Agents (DEAs) the most current full escrow file for purposes of cross referencing and confirming consistency of the domain name count in the top-level domain (TLD) to the domain name count in the TLD's zone file and bulk registration data access (BRDA) file. Additionally, the registration data for a sample of domain names is extracted from the escrow file for comparison to the information displayed by the registry operators' Whois services for the same domain names. The files are transferred to ICANN by the DEA in its encrypted format, decrypted by ICANN and encrypted for download and decryption by ICANN's audit vendor. The registry operators subject to audit are informed that ICANN will be requesting the escrow files from their DEAs. Neither ICANN Contractual Compliance, nor the audit vendor, uses the escrow file for other purposes or retains the escrow files. The audit vendor deletes the files upon the audit's completion.*

*As for registrars, ICANN Contractual Compliance requests registrar DEAs to perform periodic reviews of the contents of registrar data escrow files to ensure they are meeting the requirements of the Registrar Data Escrow Specifications. ICANN does not request or receive the escrow file in conjunction with these reviews.*

**2. ICANN Compliance to provide more specificity regarding necessary retention periods, and the rationale for retention after the domain registration is deleted. This information is necessary to justify any retention period to a DPA. Providing use cases where registration data is needed after the registration expiration would be helpful to explain relevant retention periods.**

*Upon conducting a manual review of a limited number of complaints processed by ICANN Contractual Compliance, the team found examples of complaints regarding domain names that had been deleted or transferred from a prior registrar in the following time periods before the complaints were filed with ICANN: over 6 months, 22 months, 2 years, 3 years, 4 years, 5 years and 9 years. In all examples, the registrars were able to provide the information and data that was subject to the Registrar Accreditation Agreement's two year data retention requirement and requested by ICANN Contractual Compliance. These complaints appeared in a variety of complaint types, including domain renewal, transfer and UDRP.*

*Additionally, regarding ICANN Contractual Compliance's retention period, the team has been asked by multiple policy development working groups and review teams over the years to provide historical data and additional granularity regarding its processed complaints,*

*including data from several years prior and data which requires manual review of complaint content. This is only possible where the complaints and data continue to be accessible.*

**3. Is there a date limit for ICANN accepting a complaint or request to audit regarding a registration that has been deleted? If not, what is the case of the longest period of a deleted registration that was accepted and acted upon?**

*There is no date limit regarding a registration's deletion or transfer for purposes of ICANN accepting a complaint or conducting an audit. However, in the processing of complaints and audits, ICANN does not require contracted parties to demonstrate compliance via provision of data that is not required to be retained beyond the period defined by the ICANN agreements and policies (or waiver, if applicable). As noted above in response to item #2, there is at least one example of a complaint being filed with ICANN Contractual Compliance over nine years after the domain name was transferred from the registrar which was the subject of the complaint.*

**4. In a follow up conversation with leadership, the question was raised why admin and tech fields are listed as required data elements. Is this because from the perspective of compliance these data fields must be collected or is the ask here that IF these data elements are provided by the RNH, then compliance should be able to access this information if/when needed?**

*Both. Registration data regarding Admin and Tech contacts is required to be collected, stored and displayed by the ICANN agreements. Additionally, there are other policies which may require action by the contracted parties with respect to these contacts (e.g., the Whois Data Reminder Policy and the Transfer Policy). Therefore, in enforcing these agreements and policies, ICANN Contractual Compliance requests and processes this data.*

Email to [maguy.serad@icann.org](mailto:maguy.serad@icann.org) from Trang Nguyen on 1 October 2018

**1. ICANN Compliance to provide completed data elements workbook for purpose F, with specific focus on which data elements are required for compliance functions (for both audit and complaint handling), as well as how long should registrars/registries retain registration data for the purpose of ICANN Org compliance audits/complaints.**

*ICANN Contractual Compliance's completed worksheet for Purpose F was provided to the EPDP policy team by Trang Nguyen via email on 3 October 2018.*