

Summary of ICANN Organization's Contractual Compliance Team Data Processing Activities

The ICANN Contractual Compliance Team processes personal data through the gTLD Registry Compliance Program, the Registrar Compliance Program, and the Compliance Audit Program. These programs ensure that contracted parties comply with all requirements in their agreements with ICANN organization and the applicable ICANN consensus polices.

1. Compliance Tickets

The Contractual Compliance Team ensures compliance with contractual obligations through the processing of compliance tickets.

Personal Data Processed: The following types of personal data are processed for compliance tickets, where applicable: (i) the contact information (name, organization, email address, telephone number, mailing address) of the complainant and complainant's representative(s); (ii) the publicly available WHOIS data of the relevant domain name registrant; (iii) the redacted registration data of the relevant domain name registrant; (iv) the contact information (name, organization, email address, telephone number, mailing address and conflicts of interest information) of the ICANN approved Public Interest Commitment Dispute Resolution Procedure (PICDRP) panel members in the context of processing compliance tickets; (v) the contact information (name(s) and email address(es)) of ICANN approved Data Escrow Agents (DEAs) and DEA's representative(s); and (vi) the contact information (contact name(s), telephone number(s), mobile number(s), email address(es), mailing address, and fax number) of the representative(s) for the contracted party.

Processing Activities: Contractual Compliance tickets are generated through the following channels: (i) web forms at <https://www.icann.org/compliance/complaint>; (ii) email submission; (iii) the WHOIS Accuracy Reporting System (ARS) Project; (iv) the Bulk WHOIS Complaint Submission Tool; and (v) referrals by Contractual Compliance Team or other internal ICANN org members.

Tickets are categorized and processed by complaint type through an ICANN hosted tracking system. Tickets that are generated from web form or email contain the complainant's contact information to facilitate the resolution of the complaint. Where a specific domain name is at issue in a complaint, the Contractual Compliance Team queries the publicly available WHOIS data through a WHOIS lookup tool or Port 43 to help validate whether the issue(s) outlined in the complaint are within scope of the Registry Agreement, Registrar Accreditation Agreement, or Consensus Policies.

If the Contractual Compliance Team is unable to validate the issue(s) outlined in a complaint because the publicly available WHOIS data is redacted/masked, it will request the redacted/masked registration data directly from the contracted party (or its representative). In these instances, the Contractual Compliance Team will only request

the redacted/masked data elements that are needed to validate the issue(s) outlined in the complaint.

Once validated, the Contractual Compliance Team will engage with the contracted party (or its representative) to resolve the complaint informally.¹ As part of this engagement, the Contractual Compliance Team will share with the contracted party the relevant information submitted by the complainant as well as any relevant information gathered as part of the validation process.

If informal resolution efforts are unsuccessful, the Contractual Compliance Team will escalate the complaint to the Formal Resolution Process.² Enforcement notices sent to the contracted party during the Formal Resolution Process will be published on the Contractual Compliance Notices webpage at <https://www.icann.org/compliance/notices>.

Incidental to the compliance process, the Contractual Compliance Team also receives personal data not relevant to the complaint. This information is voluntarily supplied by individuals submitting the complaint, or by the contracted party (or their representative(s)).

Legal Basis: The legal basis for the above described processing activities is legitimate interest pursuant to Article 6(1)(f) of the GDPR.

2. The Contractual Compliance Audit Program

The Contractual Compliance Team ensures compliance with contractual obligations through audits.

Personal Data Processed: The following personal data are processed for the audit program where applicable: (i) the publicly available WHOIS data of the selected domain names; (ii) the redacted registration data of the selected domain names; (iii) the contact information (name(s) and email address(es)) of ICANN approved DEAs and DEA's representative(s); and (iv) the contact details (contact name(s), telephone number(s), mobile number(s), email address(es), mailing address, fax number) of the representative(s) for the contracted party.

Processing Activities: The Contractual Compliance Team performs an audit up to twice a year for each contracted party to ensure contracted parties' compliance with their agreements and the consensus policies. ICANN org contracts with an audit firm to perform portions of the audit. In some cases, ICANN org works with DEAs to audit data escrow deposits. For further details about the processing activities performed as part of the Contractual Compliance Team's prior audits, please refer to the Audit Program webpage at <https://www.icann.org/resources/pages/audits-2012-02-25-en>.

¹ See Contractual Compliance Approach and Process webpage, *available at* <https://www.icann.org/resources/pages/approach-processes-2012-02-25-en>.

² See Contractual Compliance Approach and Process webpage, *available at* <https://www.icann.org/resources/pages/approach-processes-2012-02-25-en>.

Legal Basis: The legal basis for the above described processing activities is legitimate interest pursuant to Article 6(1)(f) of the GDPR.

3. Retention

ICANN org recognizes that the retention of personal data related to the above activities must be compliant with Articles 5(e) and Article 17 of the GDPR, among other related obligations affecting the retention of personal data. To address personal data deletion requirements under the GDPR, ICANN org has developed and implemented (i) a data deletion procedure for determining when personal data must be deleted per the GDPR, (ii) protocols and response processes for handling data subject's requests under the GDPR, and (iii) ICANN org staff awareness training of GDPR obligations. For example, the information obtained by the Contractual Compliance Team during an audit is retained by the Contractual Compliance Team until the conclusion of the audit or until the resolution of all issues related to the audit, whichever occurs later.

4. Cross-Border Transfers

ICANN org has instituted appropriate safeguards for the protection of the personal data being transferred to any third party (including cross-border transfers). Where there is a cross-border transfer within ICANN org related to these activities, such transfers are subject to technical, administrative, and organizational measures of protection designed to safeguard the data against improper or unlawful processing, including the implementation of technical controls designed to secure such personal data. ICANN org acts as a controller directly subject to the GDPR with respect to the processing of personal data associated with the above described Contractual Compliance Team activities. Where the cross-border transfer involves the use of data processors, such transfers are done in accordance with Article 28 of the GDPR, as applicable. ICANN org continues to evaluate its processing operations to ensure its continued compliance with the GDPR with respect to any cross-border transfers of personal data.