

originally sent 19 December 2018
resent 4 February 2019, for publishing

Dear Maguy:

Tucows (through its subsidiary Enom, IANA ID 48) has been working with your team for some time regarding a matter of contract interpretation. As previously indicated by the RrSG, ICANN Contractual Compliance's interpretation of a mutual contract is not the only valid interpretation—Contracted Parties have a say, too.

In this particular case,¹ Tucows implemented the Change of Registrant (COR) process² in a manner that, we believe, respects the intent of the COR policy, namely: protecting Registrants. We consider that a material update to registrant information, regardless of whether that information is public in the Whois, is sufficient to trigger COR.³

ICANN Contractual Compliance has indicated both that we must not trigger COR when the information is not public due to Whois privacy,⁴ and that we must trigger COR when the information is not public due to GDPR shielding.⁵ This creates a conflict for us; we need one uniform way to handle COR triggers for all domains. Either we trigger COR when the underlying data that we hold is updated, which would mean triggering COR both for

¹ ICANN Contractual Compliance case number NYG-645-68744, regarding domain name habinc.com.

² Transfer Policy, Section II. Inter-Registrant Transfer (Change of Registrant). <https://www.icann.org/resources/pages/transfer-policy-2016-06-01-en>.

³ Transfer Policy Section II (A) 1.1 defines a change as a "Material Change" to "Prior Registrant name" (and others). Registrant name is information that may or may not be public in the Whois but which the registrar of record will have access to. ICANN has already accepted that turning Whois privacy (proxy does not factor in, here, since there is a designated agent between the registrant and their domain name) on or off does *not* trigger the COR, indicating that it truly is the name of registrant, not the name public in the Whois database, whatever that might be.

About Change of Registrant <https://www.icann.org/resources/pages/ownership-2013-05-03-en>: "[R]egistrars must impose a lock that will prevent any transfer to another registrar for sixty (60) days following a change to a registrant's information." We understand this to mean precisely what it says, "a change to a registrant's information"; this information may only be visible to us, the registrar of record, for any number of reasons, but it remains "a registrant's information" and thus, "a change to" it will trigger a COR.

⁴ Email from Compliance dated 5 December 2017:

ICANN notes that your registrar considers any change to registrant data, even data behind a proxy service, to be a Change of Registrant (COR) under the Transfer Policy.

ICANN further notes that Section 1.3 of the Specification on Privacy and Proxy Registrations of the 2013 Registrar Accreditation Agreement (RAA) states that Proxy Service is the Registered Name Holder (RNH). The COR in the Transfer Policy only applies to certain material changes to the RNH (or Administrative Contact email address) and does not reference changes to a privacy or proxy service customer's contact information.

We note that the policy states "registrant" and not "Registered Name Holder".

Email from Compliance dated 17 January 2018:

During the call, ICANN clarified that Registrar should not lock implement 60 days inter-registrar transfer lock when there is no material change to the fields in public Whois, listed under Section II.A.1.1 of the Transfer Policy.

⁵ Email from Compliance dated 24 October 2018:

The COR lock process does not apply to changes to underlying Privacy or Proxy customer information (since it does not appear in the Whois). Nor does the COR lock process apply to changes to Temporary Specification redactions of registration data in Whois.

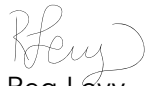
domains masked by GDPR protections and for domains with a Whois privacy service when their underlying registration data is updated, or we trigger COR only when the public-facing data is updated. No one from ICANN Contractual Compliance has been able to articulate how they propose that we resolve this conflict, nor do they have a coherent response for how this conflict exists. To be as clear as possible, we find it absurd that Compliance feels that Registrants using privacy services should not have the benefits of the COR procedure.

In addition, we have performed an informal survey of other registrars, to see how they implement COR and whether it is a model we could adopt, in order to bring ourselves into compliance with ICANN Contractual Compliance's contradictory interpretation. We have discovered that our implementation and understanding of COR is the norm.⁶

Finally, we note that, as the Transfer Policy is silent on whether or not registrant data must be public to be relevant, the Board has issued a deferral of enforcement.⁷

We respectfully submit that we have attempted to work with ICANN Contractual Compliance regarding our implementation of our contractual duties to no avail. We ask that you close this ticket, accepting that we are at an impasse and that there is no breach, merely a difference of opinion about how to best protect registrants and a divergence of opinion regarding contractual requirements that are vague.

Sincerely,
Reg



Reg Levy
Director, Compliance
Tucows, Inc.

cc: Jamie Hedlund, SVP, Contractual Compliance & Consumer Safeguard and Managing Director - Washington D.C. Office

⁶ We note that we flagged in this in our correspondence of 19 January 2018:

We [...] consider ICANN's interpretation—as stated on the call—[...]as] a major departure from previous policy interpretations within the community[.]

⁷ Adopted Board Resolutions, Regular Meeting of the ICANN Board 03 Feb 2017; resolution H: GNSO Council Request: Compliance with Inter-Registrar Transfer Policy Part C (IRTP-C) <https://www.icann.org/resources/board-material/resolutions-2017-02-03-en#1.h>