RrSG Approach to Registration Data Accuracy

February 2024

Contents

What Registration Data Accuracy means

Why Registration Data Accuracy is important

Accuracy obligations

- ICANN Policy obligations
- Legal obligations

What Registrars do to achieve and improve Accuracy

Registrar perspective: third-party validation methods

- Address validation services
- Online mapping services
- Postal Service verification

Registrar perspective: Identity verification

- Cost-effectiveness of identity document review
- Liability of the approver
- Accessibility, equity, and legal concerns

What about DNS Abuse?

What Registration Data Accuracy means

The RrSG understands Registration Data Accuracy to mean that the registration data elements provided by the Registered Name Holder or Account Holder are "syntactically accurate", and either the telephone number or the email address are "operationally accurate."

To be considered "syntactically accurate", the **validation** requirements of the Whois Accuracy Program Specification Sections 1b-d must be met. For example, for email addresses all characters must be permissible, the "@" symbol is required, and there must be characters before the "@" symbol.

To be considered "operationally" accurate", the **verification** requirements of the Whois Accuracy Program Specification Section f must be met. For example, an email sent to the Registered Name Holder must receive an affirmative response.

The Registration Data Accuracy Scoping Team Write-Up (PDF) provides a description of how these existing accuracy requirements are **understood and enforced**:

> Under the current requirements, as spelled out in the Registrar Accreditation Agreement (RAA) as well as Consensus Policies, domain name registration data should be accurate, reliable, and up-to-date. Accuracy requirements are understood as entailing syntactic validation of the registration data elements provided by the Registered Name Holder or Account Holder as well as the verification of operability of either the telephone number or the email address.
>
> To be determined to be syntactically valid, the contact must satisfy all requirements for validity (see Whois Accuracy Program Specification Sections 1b-d). For example, for email addresses all characters must be permissible, the "@" symbol is required, and there must be characters before the "@" symbol.
>
> To be determined to be verified as operable, the contact must be operable as defined in the Whois Accuracy Program Specification Section f including an affirmative response from the Registered Name Holder for either email or phone.
>
> In addition, upon notice of an alleged inaccuracy or if the Registrar learns of inaccurate contact information, the Registrar must take reasonable steps to investigate that claimed inaccuracy and to correct inaccuracy. Additional verification procedures apply if the registrar has any information suggesting that contact information is incorrect. If a Registered Name Holder willfully provides inaccurate or unreliable

registration data information, the registrar will take additional action to terminate, suspend or place a registration on hold.

Whilst there are no explicit provisions in the Base Registry Agreement that refer to the accuracy of registrant data, some specifications to the Registry Agreement relating to eligibility requirements and auditing obligations in certain gTLDs may inform the topic of registration data accuracy.

Why Registration Data Accuracy is important

Maintaining accurate and up-to-date domain name registration data allows registrars to:

- Meet legal, contractual, and policy obligations
- Send the domain owner important mandatory notices such as renewal reminders
- Contact the domain owner when problems arise, such as a compromised domain being used for DNS Abuse

Accuracy obligations

Registrars have obligations relating to registration data accuracy both in ICANN contract and policy and in relevant jurisdictional laws.

ICANN Policy obligations

The Registrar Accreditation Agreement (RAA) provides requirements for the registration agreement that domain owners enter into with their domain registrar, including specific requirements relating to domain name registration data.

- Domain owners are obligated to provide accurate and reliable contact details to the registrar, and update their contact info within 7 days of any change.
- This includes the domain owner’s name, email address, phone number, and postal address.
- If the domain owner purposely provides inaccurate or unreliable information, or does not update their data within 7 days of any change, or does not respond to verification requests within 15 days, then the domain must be suspended or canceled.

The Whois Accuracy Program Specification (WAPS) of the RAA provides detailed requirements for validating and verifying the accuracy of domain name registration data, and for disabling domain names when the data is not validated and verified within 15 days of being first provided or updated.

- If a domain's data is not validated (all required info is provided; data is in the correct format for the field) and verified (affirmative response from the point of contact, such as following a link to a website) within the required timeframe, then the domain is suspended and related services may not function until that validation and verification are complete.

The Restored Names Accuracy Policy sets requirements for registration data updates in cases where a domain was deleted due to inaccuracy.

- The policy is: "When a registrar restores a name (from the redemption grace period) that had been deleted on the basis of submission of false contact data or non-response to registrar inquiries, the name must be placed on Registrar Hold status until the registrant has provided updated and accurate Whois information."

The Whois Data Reminder Policy requires registrars to show domain owners their registration data and remind the registrant that they are required to provide accurate data.

- The policy is: "At least annually, a registrar must present to the registrant the current Whois information, and remind the registrant that provision of false Whois information can be grounds for cancellation of their domain name registration. Registrants must review their Whois data, and make any corrections."

Legal obligations

Registrars operate in jurisdictions around the world, and so each individual registrar will need to determine the legal requirements relating to data accuracy which are relevant to their particular jurisdiction(s).

The GDPR is a European data protection law which came into effect in 2018. It includes data processing principles relating to accuracy, and gives data subjects the right to rectification, allowing them to require data controllers to correct any inaccurate personal data.

NIS2 is a Directive which will be implemented into EU member-state law by October 2024. It aligns with existing practices for the accuracy of registration data. The RrSG recently sent a letter to the European Commission's Network and Information Systems (NIS) Cooperation Group Work Stream for Article 28 detailing the correspondence between ICANN obligations and NIS2 requirements and supporting ICANN's similar letter. With this context in mind, for EU registrants it will be important to record the method which was used for validating a contact as well as the exact time stamp and a verification reference (such as a ticket number). Data protection legal obligations remain in effect, so additional document validation may be deemed excessive or unnecessary to fulfill the initial purpose for processing.

What Registrars do to achieve and improve Accuracy

Registrars have multiple tools at hand to ensure that registration data provided by the domain owner remains accurate and up-to-date.

Scorecard Legend:
✅ = yes = 1 point
❓ = maybe/unknown = ½ point
❌ = no = 0 points

Validate and verify

Registrars must validate and verify registration data as described in the Whois Accuracy Program Specification. This process is triggered by specific changes to a domain name including new registration, transfer to a new registrar, or change to the registered name holder; if the data is not verified within a limited period of time, use of the domain is suspended until the verification is complete.

When validating, the registrar must ensure that all required fields are populated and that data matches required publicly-available formatting standards; for verification, the registrar must contact the domain owner by email or telephone and receive an affirmative response.

This process allows the registrar to ensure that all required data has been collected, and to confirm that the provided data is accurate, reliable, and up-to-date.

Scorecard:
✅ Global scope
✅ Cost-effective
✅ Reliable
Total: 3/3

Above and beyond: additional verification

Additional verification of the accuracy of provided registration data can be supported by developing accuracy dashboards and tools that leverage open source databases and APIs.

These tools can help confirm if a postal code matches the city or has the right format, or whether a street number actually exists on the street. Family and given names can be checked if they match a certain syntax and length, and to ensure they do not contain words such as "Hostmaster" or "Domain Admin" which typically are not family names. This is complicated by potentially confusing names, such as the surname “Contractor” (*this is a real-life example!*) For businesses, there are likely public databases to confirm their validity.

Scorecard:
✅ Global scope
❓ Cost-effective
❓ Reliable
Total: 2/3

Registrar perspective: third-party validation methods

Registrars operate global businesses, and so any solutions for registration data accuracy must be similarly global in scope, relatively cost-effective, and reliable.

Address validation services

One potential method to confirm registrant information is through address validation using third party services. These are frequently used by shipping companies (e.g. FedEx) or ecommerce sites (e.g. Amazon).

While these services can provide accurate data, they are limited to the countries in which the companies which own them operate. Because a functional delivery address is the most important component of an order for such companies (after payment), they can invest significant resources into developing these systems. In many cases, the consumer pays a shipping fee which includes an element of cost-recovery for these systems.

Scorecard:
❌ Global scope
❓ Cost-effective
✅ Reliable
Total: 1.5/3

Online mapping services

Another potential method to confirm accuracy is online mapping services such as Google Maps. As with the other third party services, Google Maps is not globally comprehensive, nor is it authoritative, as addresses may appear within its database despite not being valid postal mail addresses. Correcting those invalid addresses can be extremely difficult to achieve, resulting in unreliable service overall.

Scorecard:
❌ Global scope
❓ Cost-effective
❌ Reliable
Total: 0.5/3

Postal Service verification

Some postal services provide address verification systems. Since this is not offered by all postal services worldwide, and there is no centralized API, any registrar intending to use a postal service system would need to dedicate significant software development to integrate with each different postal service's API.

Even if a postal address verification system confirms that the address is valid, this type of check cannot confirm whether the person claiming the postal address is actually contactable at that address. This would instead require additional verification, such as sending postal mail addressed to them or visiting in person and performing some type of confirmation process, which adds potentially significant financial cost, and causes significant and unnecessary delays in the use of the domain.

The UPU review of postal addresses during the Whois ARS found that 99% of postal addresses sampled had deliverable addresses, suggesting that postal address inaccuracy in registration data is not a problem in need of a solution.

Scorecard:
❌ Global scope
❌ Cost-effective
❌ Reliable
Total: 0/3

Registrar perspective: Identity verification

Identity verification based on government-issued identification documents is difficult in part due to the high complexity and sophistication required to accurately validate the identity, and in part due to concerns around accessibility, equity, and legality.

Cost-effectiveness of identity document review

There is significant diversity of types of worldwide identification documents, and so registrars typically require the services of third-party vendors to verify these documents. This brings new costs, which if conducted for all registered domains would significantly impact pricing. In 2021, ICANN estimated that identity verification on a global scale would cost $10 to $20 USD per check. While less-expensive identity verification services may exist, these do not offer global coverage.

Liability of the approver

There is also a liability concern: if the validation is completed incorrectly then either a genuine registrant was denied their domain name or a false document was used to complete the verification, either way a problem. There may also be deleterious effects on the initial holder of the identity document, if it was stolen and used to register a domain which itself is used for illegal activity.

Accessibility, equity, and legal concerns

Not everyone has identification documents; requiring the display of identification documents disproportionately adversely affects marginalized communities who lack government-issued identification.

Registrars should not evaluate the legitimacy of identification documents. As we already discussed, in a global economy there is no scalable way for support staff to know the requirements of each type of identity document they may be presented with, and incorrect conclusions may create legal liabilities, especially with new AI-generated documentation that is impossible to discern from real documents. Additionally, some identification documents are not permitted to be used for other purposes (such as validating the identity of the holder for an online purchase), but the domain owner may not know that or may feel they must choose between following that law or registering a domain name.

Further, reviewing identity documentation is a data processing activity which goes well beyond the minimum required to offer the service; as we've seen for years it is certainly possible to register a domain without sharing one's identity documentation. This may bring the registrar into conflict with legal obligations relating to data minimization.

Validating identity documents from only some (but not all) jurisdictions could also result in bad actors purposely using documentation from non-validated locations. This means that honest registrants are faced with excessive and unnecessary data processing while dishonest abusers of the system go uncaught, having found a workaround to even the most stringent identity validation process.

Scorecard:
❌ Global scope
❌ Cost-effective
❌ Reliable
Total: 0/3

What about DNS Abuse?

There are some specific ccTLDs that require identity verification; those are associated with countries which use unified identity documentation for the entire country.

Even with verification processes in place, there is no clear evidence that these verification systems are effective at preventing abuse; TLDs with these requirements, even those that are fully verified, often appear on “Top 10 Most Abused TLD” lists.

There is, however, emerging evidence that these identity document verification systems can be circumvented through the purchase of false verifications or documentation.

In the absence of evidence demonstrating either a problem with the accuracy of existing registration data or a benefit (such as disrupting or mitigating DNS Abuse) gained through additional validation and verification processes, these drawbacks have led to registrars not adopting these identity verification services.