

**The three questions posed to ICANN Org are:**

- 1) What current and near-term legislative efforts could affect the requirements for registrants to maintain accurate registration data?
- 2) What current and near-term legislative efforts could affect the requirements for contracted parties to maintain accurate registration data?
- 3) Is there any legislation currently implemented or anticipated that could trigger a PDP or EPDP to evolve ICANN policy or contracts related to mandatory accuracy?

---

**ANSWERS:**

Since the responses to both questions regarding the requirements for registrants and contracted parties to maintain accurate registration data are closely linked, they will be addressed jointly in the response below.

For the avoidance of any doubt, by "current and near-term legislative efforts," we are referring to recent or upcoming laws, regulations, or directives that are in the process of being implemented or are expected to be enacted soon, which could impact how registrants and contracted parties are required to handle and maintain accurate registration data. The response below does not cover existing legislation, such as the accuracy requirements outlined in the General Data Protection Regulation (GDPR), which have already been implemented.

The answers provided below reflect information from the Government Engagement (GE) team of ICANN, which monitors legislative and non-legislative initiatives that may impact ICANN's mission and policies. These answers do not constitute a legal analysis. While GE tracks the most significant legislative developments globally, there may be other legislative initiatives in various regions that we are not yet aware of or are currently monitoring.

## 1. Q1&2: Requirements for Registrants and Contracted Parties to Maintain Accurate Registration Data

A key recent and upcoming legislative development that may influence how registrants and contracted parties are obligated to manage and maintain accurate registration data is the NIS2 Directive (Network and Information Systems Directive 2), which is currently being implemented in the EU. The NIS2 Directive, along with the recommendations for its implementation issued by the NIS Cooperation Group, and the national laws of EU Member States transposing the Directive into their own legal frameworks, will be examined below in relation to the requirements for the accuracy and verification of registration data.

The NIS2 Directive ([EU\) 2022/2555](#) (Directive on measures for a high common level of cybersecurity across the European Union) was adopted in November 2022, replacing the previous Directive (EU) 2016/1148. As a legislative act, a directive establishes a common objective for all EU countries to achieve, but it is up to each country to implement its own laws to meet that objective. EU Member States were given a deadline of 17 October 2024 to transpose the provisions of NIS2 into their national laws. To date, only 4 Member States—Belgium, Lithuania, Italy and Croatia—have transposed the NIS2 Directive. The European Commission has initiated [infringement proceedings](#) on the remaining 23 Member States for failing to comply with the deadline.

### *a. NIS2 Directive Requirements for Accuracy in Registration Data and ICANN Policies and Procedures*

The NIS2 Directive establishes obligations about registration data collection, maintenance and disclosure “for the purpose of contributing to the security, stability and resilience of the DNS”, “which in turn contributes to a high common level of cybersecurity within the Union”. It applies to both ccTLD and gTLD name registries and entities providing domain name registration services (registries and registrars) that are established in the EU or offer services in the EU, hence having an extraterritorial scope of application.

According to Art. 28(3) of the NIS2 Directive “Member States shall require the TLD name registries and the entities providing domain name registration services to have policies and procedures, including verification procedures, in place to ensure that the databases referred to in paragraph 1 include accurate and complete information. Member States shall require such policies and procedures to be made publicly available.”

The term “accuracy” is not defined in the NIS2 Directive nor are the “verification procedures” mentioned in Art. 28(3).

Recital 111 sets out comparatively specific and dynamic requirements regarding verification obligations and may become a ‘moving target’ in the future as best practices and available tools evolve. Verification processes of TLD registries and the entities providing domain name registration services “should reflect the current best practices used within the industry and, to the extent possible, the progress being made in the field of electronic identification”. This recital also provides general examples of verification processes, which “may include both ex ante controls, performed at the time of the registration, and ex post controls, performed after the registration”. In particular, TLD registries and the entities providing domain name registration services are required to verify at least one means of contact of the registrant.

While NIS2 introduces new legislative requirements for DNS operators, its accuracy and verification provisions largely reflect what has already been required by ICANN’s existing policies. Specifically, the Registrar Accreditation Agreement’s (RAA) RDDS Accuracy Program Specification requires that registrars validate, inter alia, that email addresses (Section 1(b)), telephone numbers (Section 1(c)), and postal addresses (Section 1(d)) are in the proper format. Furthermore, the Specification requires registrars to verify that either the registrant's email address (Section 1(f)(i)) or telephone number (Section 1(f)(ii)) are operable.

*b. NIS Cooperation Group Work Stream for Article 28 guidance and European Commission Recommendation on measures to combat counterfeiting and enhance the enforcement of intellectual property rights*

The NIS Cooperation Group Work Stream for Article 28, set up to promote cooperation and information exchange among Member States, the European Commission and the European Union Agency for Cybersecurity (ENISA) on the article’s implementation, has issued on 18 September 2024 [non binding guidance](#) for Member States to consider as they transpose this article of the directive. The Work Stream focused on the verification and access of registration data, and on the need to establish a methodology combining a risk-based approach with the operational verification of registration data. The NIS Cooperation Group Work Stream recommends the contact email address and the telephone number of the registrant are both syntactically validated and operationally verified for both new domain registration and the renewal of existing domains. It also recommends methods for identity verification (either through third parties, own verification or mixed) should be in place for both natural and legal entities. Electronic

identification should be the preferred means anytime it is available in the respective Member State and for the category of registrant.

Furthermore, it is worth noting that on 19 March 2024 the European Commission published a [Recommendation on measures to combat counterfeiting and enhance the enforcement of intellectual property rights](#). Under the heading “*Domain names providers: Ensuring the protection of IP rights in the Domain Name System*”, TLD name registries and entities providing domain name registration services established in the EU and/or offering services in the EU are encouraged to implement the following good practices among others:

- *to provide for verification procedures for domain name registration data, by using, e.g. electronic identification solutions and/or publicly accessible registers such as civil and commercial registers to verify the identity of the registrant in full compliance with the right to data protection;*
- *to take voluntary measures to detect incorrect registration data for existing domain names, and to give registrants a reasonable time period to correct or complete such data, after which a notice of suspension of the delegation of their domain name may be given.*

Although the NIS2 Directive is not prescriptive with respect to the methods to verify at least one means of contact of the registrant (“should reflect the best practices used within the industry and, to the extent possible, the progress made in the field of electronic identification” Rec. 111), the NIS Cooperation Group Work Stream for Article 28 guidance and the European Commission’s Recommendation on measures to combat counterfeiting and enhance the enforcement of intellectual property rights set a high standard for the potential technology to be employed. Both the NIS Cooperation Group Work Stream for Article 28 guidance and the European Commission’s Recommendation on measures to combat counterfeiting and enhance the enforcement of intellectual property rights are nevertheless non-binding.

As noted above, only 4 Member States have transposed the NIS2 Directive. Therefore, we must wait for the implementation laws of the remaining 23 EU Member States to determine the potential impact on ICANN policies and the ICANN multi-stakeholder model.

### *c. National Implementation of NIS2 Directive in EU Member States*

Below is language from how Belgium, Lithuania, Italy and Croatia have transposed the accuracy and verification requirements of the NIS2 Directive.

#### **Belgium**

## **[Chapter 2, Article 94, Paragraph 2](#)**

The top-level domain name registries and entities providing domain name registration services shall have policies and procedures, including verification procedures, to ensure that the databases referred to in paragraph 1(1) contain accurate and complete information. These policies and procedures shall be made publicly available.

If the domain name registration details listed in paragraph 1(2) of a domain name are false, inaccurate or incomplete, the registries for top-level domain names and entities providing domain name registration services shall immediately block the operation of such domain name until the domain name holder corrects the registration details so that they become true, accurate and complete. If the domain name holder fails to do so within the time limit set by the Registry for Top Level Domain Names or by the entity providing domain name registration services, the domain name will be canceled.

The transfer of a blocked domain name to another entity providing domain name registration services is prohibited.

## **Lithuania**

### **[2024 m. liepos 11 d. Nr. XIV-2902 - Article 17, Paragraph 2](#)**

Cyber security entities that are entities providing top-level domain name registration services and entities providing domain name registration services must [...] (2) implement policies and procedures, including verification procedures, to ensure that the domain name registration database contains accurate and complete information;

## **Italy**

### **[DECRETO LEGISLATIVO 4 settembre 2024, n. 138, Chapter 4, Article 29, Paragraph 3](#)**

Managers of TLD Registries and providers of domain name registration services shall establish and make public policies and procedures, including verification procedures, to ensure that the databases referred to in paragraph 1 contain accurate and complete information.

## **Croatia**

Content of information in databases on domain name registration and identification of domain users

### **§ 46**

(2) The registry of top national Internet domain names and registrars are obliged to determine the identity of the domain user and verify his identity on the basis of identification documents, i.e. documents, data or information obtained from a credible, reliable and independent source, including, if the domain user has one, a qualified certificate for an electronic signature or electronic seal or any other secure, remote or electronic, identification procedure regulated, recognized, approved or accepted by the relevant national authorities.

(3) Non-compliance by applicants for domain registration and domain users in accordance with the obligations prescribed by this Law is the basis for denial of domain registration, i.e. deletion of the domain.

Obligations of the registry of national Internet top-level domains and registrars

### **§ 47**

(4) The registry of top-level national internet domain names and registrars are obliged to establish and publicly publish the database management policies from Article 46 of this Act, which must also include data verification procedures from domain registration requests.

To conclude, as regards current and near-term legislative efforts that could affect the requirements for registrants to maintain accurate registration data or affect the requirements for contracted parties to maintain accurate registration data, we will have to wait for the implementation laws of the remaining 23 EU Member States to determine.

## **2. Q3: Current or anticipated legislation that could trigger a PDP or EPDP**

Laws governing the domain name space are constantly evolving, and new legislation may impact existing practices. Like all laws, contracted parties are obligated to comply with the relevant legal requirements in their respective jurisdictions. As a general principle, when there is no direct conflict between legal requirements and ICANN

policies, there has been no immediate need to amend existing ICANN policies. However, regardless of legislative changes, the ICANN community has the authority to engage in discussions and implement policy modifications as deemed necessary by the community to ensure continued alignment with its objectives.

It is important to note that while ICANN org plays a key role in supporting policy development, the decision to trigger a Policy Development Process (PDP) or an Expedited Policy Development Process (EPDP) does not rest with the ICANN org itself. Instead, this decision must be carefully considered within the GNSO. While the ICANN community could decide to initiate policy development work to recommend alignment between ICANN consensus policy requirements and the requirements in the NIS2 implementing laws, in ICANN org's view, there is not a critical need to do so, because there is no direct conflict between the implementing laws and ICANN policy and contract requirements. In other words, while the implementing laws could require the contracted parties to do more than what is required per ICANN Consensus Policy, compliance with the implementing laws would not prevent the contracted parties from also adhering to the applicable ICANN Consensus Policy requirements., Further, it is still unclear what the other awaited implementing laws from the remaining 23 Member States will require. As it stands, ICANN's existing policies are largely consistent with the requirements set out in NIS2. In this context, ICANN has also prepared and submitted a communication to the NIS Cooperation Group Work Stream on Article 28, compiling the relevant existing and upcoming ICANN policies.