WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

eco

# Backgrounder on NIS2 Provisions and their Interplay with the Domain-Name-System (DNS)

Cologne, 29 November 2021

The obligation to provide regularly updated complete and verified registration data for domain names, as suggested in Article 23 of the EU's draft NIS2 Directive is excessive in eco's view and presents a considerable administrative, financial and competitive burden for the companies concerned with questionable impact on the improvement of the security, stability and resilience of the DNS. It also raises concerns in regard to existing data protection legislation. In this light, eco considers the impact of this obligation on global businesses and customers to be disproportionate and calls on the lawmaker to critically re-assess the requirements for registrars and registries of domain names and to scrutinise their added value in terms of appropriateness and proportionality when it comes to security.
The EU's draft NIS2 Directive raises particular concerns by giving the impression that the focus is particularly on registries and registrars of domain names. This current draft represents an unequal treatment compared to other identifier systems on the Internet, e.g. IP addresses and email addresses, even though they can equally be used for abusive activities.

## I. Security, Stability & Resilience of the DNS

The providers of DNS services play an important role in the security, stability and resilience of the DNS and balance these interests with the need for the protection of personal data and privacy. In order for a registrar or a registry to take action and disable domain names that are involved in DNS abuse, registration data is likely to be less valuable for law enforcement agencies than the data of the account holder, i.e. the natural or legal person that has entered into a contract with a registrar, as that data includes payment data.

Further, gTLD registries and registrars are required to publish contact details for an abuse point of contact or an emergency point of contact based on the contractual requirements in the Registration Accreditation Agreement of the Internet Corporation for Assigned Names and Numbers (ICANN). Even though there is no policy requiring such contact for ccTLD operators, these operators are also responsive to abuse notifications. An alternative reporting channel for non-EU-based providers is the NIS representative. Therefore, multiple options are already available to report DNS abuse to registries and registrars of domain names without the need for the data of the registrant.

## II. Registrant Data & Data Protection

- **Data Collection & Data Minimization**

For most domain registrations, the registration data is not collected or stored by registries but rather by registrars, resellers and privacy/proxy providers. Resellers may themselves have resellers. These 2nd-order resellers have no direct link to or contract with the registrar and the registrar may not even be aware of them. There is no limit to the depth of this reseller chain. Some or all of the registration data may never be stored by (or even presented to) the registrar. It will be held by a privacy or proxy provider. A proxy provider will share neither the name of the real registrant nor their contact information.

We would like to point out that the concept of 'verifying' database information has been expanded through the ITRE report. This implies that each party in a contractual chain will be required to conduct due diligence on the accuracy and completeness of domain name registration data. This is contrary to data minimisation principles and would oblige European registrars to undertake transfers of personal registrant data to non-EU countries under questionable legal conditions, if registries are based outside the EU.

This language regarding the required publication of data oversimplifies the idea of domain name registration data – a set of data comprises multiple different fields, each of which may or may not contain personal data, and, therefore, there are challenges with treating a single registration as either 'legal' or 'personal', e.g., a situation where the registrant's name is 'domain admin,' the organisation name is 'Example Company' but the email is FirstName.LastName@ExampleCompany.TLD'.

- **Data Verification**

As of now, contactability is verified by the registrars when the registrant positively responds to a communication issued by the registrar at the time of domain registration and, if the contact is not positively verified, the domain may be suspended or cancelled. Section 3.7.7 of the Registrar Accreditation Agreement with ICANN includes this verification requirement, which is narrowly tailored to the purpose of contactability. Registrars are concerned and are of the opinion that the further collection and processing of personal data (i.e. IDs, passport, photos) is neither necessary nor proportionate for contact verification when registering a domain name. This is again contrary to data minimisation principles.

- **Data Protection**

We thus express our concern with the current formulation that allows access to very generic 'legitimate access seekers'. The GDPR formulation of 'legitimate interest' has paved the way to very broad access to personal information. We think that access to personal information in domain name registration databases should only be granted to public law enforcement authorities under due judicial process. This would strike a balance between the intrusion into the privacy of individual registrants

and the guarantees against the misuse of their personal information.

Moreover, once accurate and verified contact information has been collected by each party in a contractual chain, it would become of utmost importance to ensure that such data is adequately protected. Given the high value of this information for identity theft and cybercrime, domain name registration databases would easily become the target of cybercriminals attacking the operator's servers to gain access to the database.

## III. Economic Impact

- **Inconsistent Implementation in EU Member States**

We are concerned that, without further guidance, the requirements broadly outlined in Article 23 of the draft NIS2 Directive have the potential to be implemented differently across different Member States, thereby imposing inconsistent and diverging requirements on TLD name registries and registrars depending on the Member State in which such entities are established and/or offer services. Such inconsistency could undermine the Commission's broader efforts to promote cybersecurity resilience across the European Union and could also have a negative impact on competition within the domain name industry.

- **Operationalisation of Verification**

European registries and registrars will be expected to do more in terms of ensuring the accuracy of the registration data they hold. This could potentially mean verifying the identity of a registrant and the accuracy of the contact details they provide before accepting a registration. Without the large-scale rollout of eIDs and digital wallets, identity verification is not straightforward and cannot be automated.

Consequently, any verification requirements would make the registration process significantly more complex and expensive for registrants. Further, registrars may not always be able to verify non-EU registrant information. Should the EU institutions decide to include verification obligations in the NIS2 Directive, we would welcome clarification on whether non-EU registrants are within that scope and what the standards of verification would be.

gTLD registrars are already required to verify certain data elements based on their Registrar Accreditation Agreement with ICANN. Registrars are the entity collecting the data from registrants. Such validation should be deemed sufficient to fulfil the requirements of NIS2. Also, the requirements laid down in the draft NIS2 do not make a distinction between the role of registries and registrars when it comes to the validation of data. Since registration data is collected by the registrar and then transferred to the registry, it would lead to a duplication of efforts if both registries and registrars were required to validate the same data elements. Additionally, an obligation to verify the identity of a registrant and the accuracy of the contact details

before accepting a registration stands again in contrast to ICANN's contractual requirements. These ensure the timely and consumer-friendly registration of domain names.

Further, not all registries obtain data on the registrants from the registrars. Operators of such 'thin whois' databases historically cannot validate data as they follow a decentralised approach and do not process any registrant data.

- **Costs & Global Competitiveness of European Registrars**

It seems that, when framing Article 23 of the draft NIS2 Directive, the European Commission has failed to take proper account of the fact that the domain name market is global – especially where gTLDs are concerned. Due to local presence, a registrant often has a strong preference for a particular ccTLD. In such cases, the registrant is likely to put up with the extra cost and efforts involved. But European registrars will not only have to comply with NIS2 requirements when registering domains under European ccTLDs, but also when registering gTLDs and non-European ccTLDs.

As a result, it could become significantly more expensive and time-consuming to register any domain name through a European registrar than through a non-European registrar. This is a highly undesirable effect on the competitiveness of registries and registrars operating under EU jurisdiction. Consequently, the draft NIS2 Directive threatens the global competitiveness of European registrars.

## IV. Overlap with other Regulations

Access to data by legitimate access seekers such as law enforcement bodies is already properly defined in the more appropriate Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (e-Evidence Regulation).

We are concerned that European regulation of the processing of registration data will put the role of ICANN into question. Through the Governmental Advisory Committee (GAC), the European Commission is actively following and involved in these processes.

Additionally, a policy development process at ICANN (EPDP on the Temporary Specification for gTLD Registration data) has recommended the establishment of a Standardised System for Access and Disclosure (SSAD), through which data disclosure requests would be processed. Diverging disclosure requirements that would need to be processed by registries and registrars would undermine the creation of such a centralised system, leading to the fragmentation and duplication of efforts.

The ITRE report introduced a call for the creation and maintenance of a registry

containing information about essential and important entities that comprise DNS service providers, including TLD name registries. This database already exists for TLD registries and is operated by the Internet Assigned Numbers Authority (IANA).

---

**About eco:** With over 1,100 member companies, eco is the largest Internet industry association in Europe. Since 1995 eco has been instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. eco's key topics are the reliability and strengthening of digital infrastructure, IT security, and trust, ethics, and self-regulation. That is why eco advocates for a free, technologically-neutral, and high-performance Internet.