EU Directive on the security of network and information system ("NIS2"): Article 28 and WHOIS

Gemma Carolillo
European Commission – DG CONNECT

DNS and domain name registration data in NIS2

Critical role of DNS recognised: “upholding and preserving a reliable, resilient and secure DNS are key factors in maintaining the integrity of the Internet and are essential for its continuous and stable operation, on which the digital economy and society depend.”

Importance of domain name registration data: “Maintaining accurate and complete databases of domain name registration data (so called ‘WHOIS data’) and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity across the Union.

Availability and accessibility of the data: “The availability and timely accessibility of these data […] is essential for the prevention and combating of DNS abuse, and for the prevention and detection and response to incidents”.

Article 28: main objectives

Contribute to increasing the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union

Establish a legal framework that ensures that the domain name registration data are accurate, complete and accessible to legitimate access seekers.

Provide a set of obligations **in relation to those objectives.** It does not prescribe a specific implementation model – leveraging existing and to be developed good practices

Domain name registration data (Article 28) – Obligations (I)

Collect and maintain accurate and complete registration data

(1) For the purpose of contributing to the security, stability and resilience of the DNS, **Member States shall require that TLD name registries and the entities providing domain name registration services collect and maintain accurate and complete domain name registration data** in a dedicated database with due diligence in accordance with Union data protection law as regards data which are personal data.

European Commission

Domain name registration data (Article 28) – Obligations (I)

Contain relevant information necessary to identify/contact holders and contact points – Specific dataset

(2) For the purpose referred to in paragraph 1, **Member States shall require the database of domain name registration data contain necessary information to identify and contact the holders of the domain names** and the points of contact administering the domain names under the TLDs. Such information shall include:

a. the domain name,

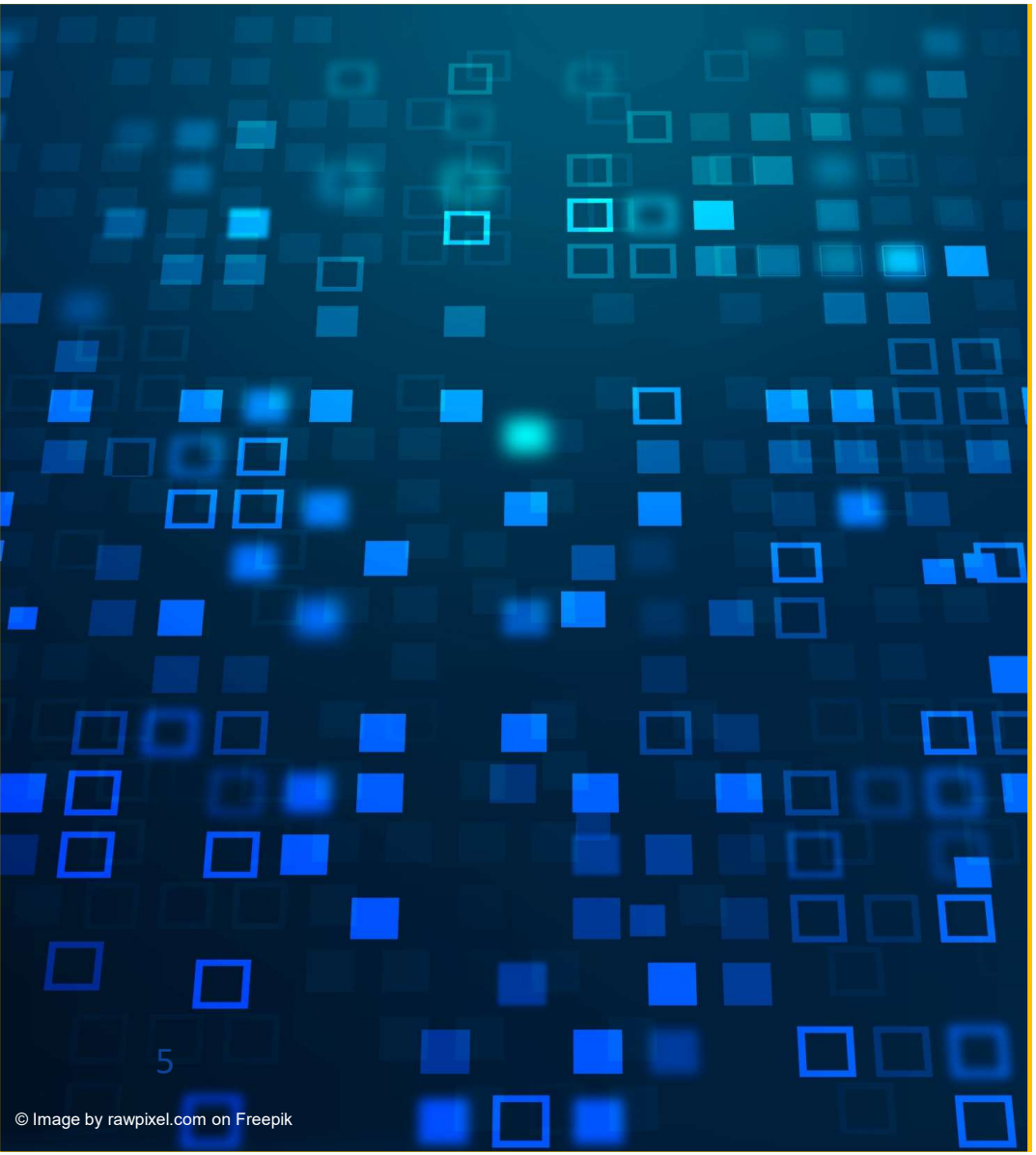
b. the date of registration,

c. the registrants' name, contact email address, and telephone number;

d. the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.

Elements for consideration

- The **objective of the provisions** → indicated in recital 109 and article 28 (1)[“the purpose of contributing to the security, stability and resilience of the DNS”] as well as recital 110 [“prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents.”]
- **Entities in scope** → TLD name registries and entities providing domain name registration services established in the EU or providing services to the EU
- **Accuracy and completeness of registration data** → it is linked to the purpose (DNS security, stability and resilience; prevent and combat DNS abuse), it does not replicate GDPR principle.
- Art. 28 NIS2 provides a **clear legal basis** for TLD registries and entities providing registration services to process the data for the specific purpose – legal obligation (art. 6(1)(c) GDPR).
- The above obligation is **without prejudice to the possibility to collect domain name registration data for other purposes**, for example on the basis of contractual arrangements or legal requirements established in other Union or national law (recital 109).



Domain name registration data (Article 28) – Obligations (II)

Need to have policies to ensure accuracy and make such policies publicly available

(3) **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 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.**

European Commission

Domain name registration data (Article 28) – Obligations (II)

Publish non-personal data, such as data concerning legal entities, without undue delay

(4) Member States shall require that the TLD name registries and the entities providing domain name registration services **make publicly available, without undue delay after the registration of a domain name, domain name registration data which are not personal data.**

Elements for consideration

- Policy and procedures should guarantee the **integrity and availability of domain name registration data**, as well as to prevent and correct inaccurate registration data,(recital 111)
- Policies and procedures should take into account, to the extent possible, **the standards developed by the multi-stakeholder governance structures at international level** (recital 111)
- **Policy and procedures should cover verification**: not a single solution. They should be proportionate, could be ex ante or ex post, they should reflect best practices and to the extent possible the progress in the field of eID. (recital 111).
- **Transparency**: all policies related to article 28 should be made publicly available.
- **Publication of non-personal data**, such as legal entities as they are outside of the scope of protection of GDPR.
  - "For legal persons, […] should make publicly available at least the name of the registrant and the contact telephone number. The contact email address should also be published, provided that it does not contain any personal data, such as in the case of email aliases or functional accounts" (recital 112).

Domain name registration data (Article 28) – Obligations (III)

Provide access to specific personal data upon duly justified requests by legitimate access seekers

+ Ensure all requests to access receive a reply within 72 hours

(5) Member States shall require that the TLD name registries and the entities providing domain name registration services **provide access to specific domain name registration data upon lawful and duly justified requests by legitimate access seekers,** in accordance with Union data protection law. Member States shall require the TLD name registries and the entities providing domain name registration services to **reply without undue delay and in any event within 72 hours of receipt of any requests for access**. Member States shall require that policies and procedures with regard to the disclosure of such data to be made publicly available.

Domain name registration data (Article 28) – Obligations (III)

Cooperation obligation

(6) Compliance with the obligations laid down in paragraphs 1 to 5 shall not result in a duplication of collecting domain name registration data. To that end, **Member States shall require TLD name registries and entities providing domain name registration services to cooperate with each other.**

European Commission

Elements for consideration

- NIS2 does not provide or prejudge what is a relevant legal basis for the access seekers: it could be in the mandate of access seekers (e.g., competent authorities), or another legal basis.
  - **Legitimate access seekers** are to be understood as any natural or legal person making a request pursuant to Union or national law.
    - They can include authorities that are competent under this Directive and those that are competent under Union or national law for the prevention, investigation, detection or prosecution of criminal offences, and CERTs or CSIRTs (recital 110).
- **The access procedure could include the use of an interface, portal or other technical tool** to provide an efficient system for requesting and accessing registration data. (recital 112)

Elements for consideration

- Member States should ensure that all types of access to personal and non-personal domain name registration data are **free of charge.** (recital 112)
- NIS2 recognizes that the DNS is a distributed system where cooperation is required to achieve the objectives:

  - **No duplication of the collection of the data** from the registrants (recital 109)
  - **Service level agreements between the parties** to deal with requests for access from legitimate access seekers to be made public (recital 112).

Thank you for your attention!

European Commission