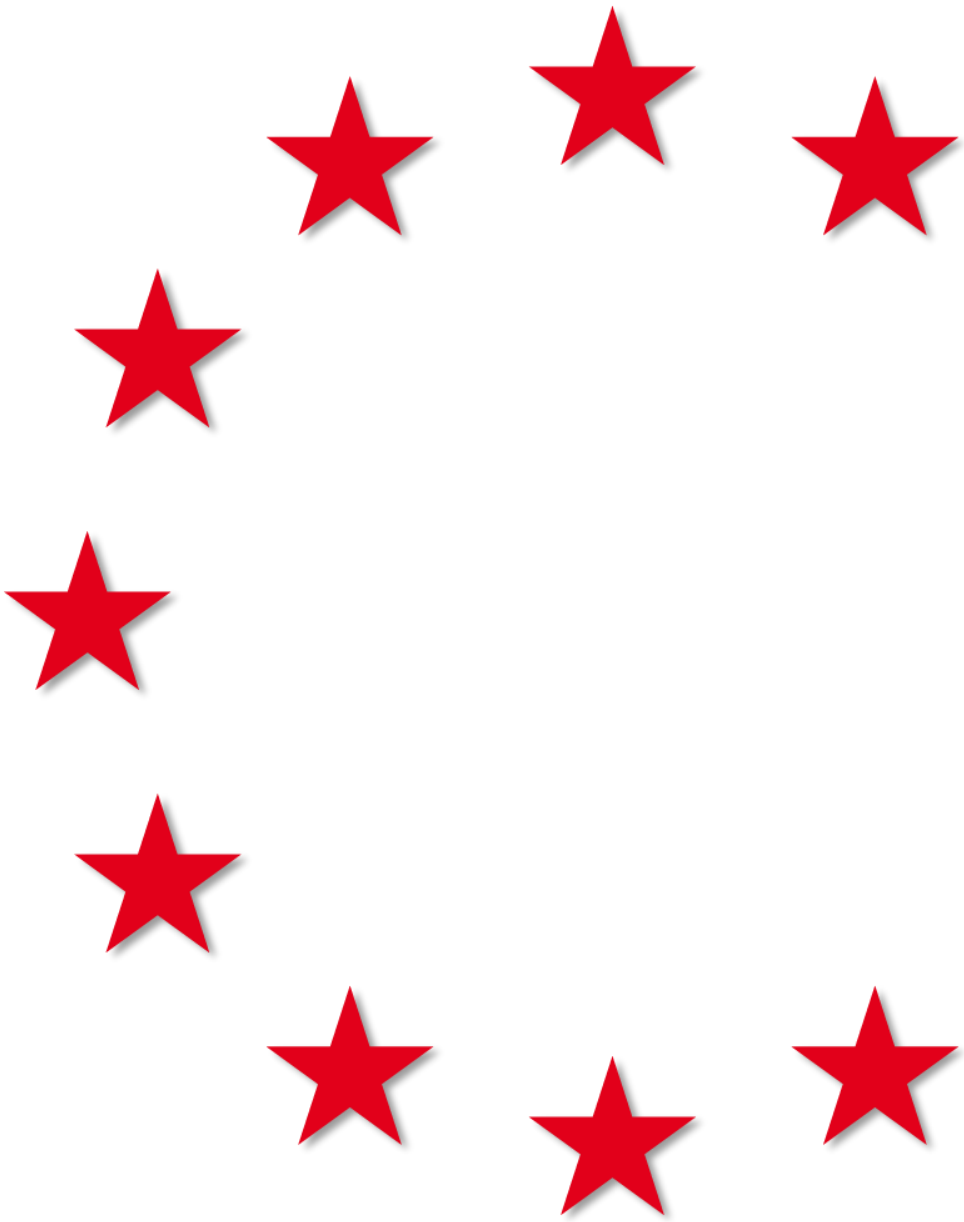
ASSOCIATION OF THE INTERNET INDUSTRY

THE NIS2 DIRECTIVE

Impact on the Domain Industry



The NIS2 Directive is the EU-wide legislation on cybersecurity. It is a set of legal measures designed to improve the overall level of cybersecurity in the European Union. The NIS2 Directive also has implications for domain name registrations in the EU and for the cybersecurity sector. Requirements for domain name registrations, in particular registration data, are set out in Article 28 of NIS2.

What makes NIS2 a challenge for the domain industry is that it comes in the form of a directive. A directive is a piece of legislation that defines a goal that all EU countries must achieve. However, it is up to each country to decide how to achieve that goal. This could potentially result in 27 different procedures for validating the data used to register a domain name. Given the fact that the domain industry is a global ecosystem of domain name registries, registrars, resellers, etc. interacting with each other, procedures like validation should be based on proven industry best practices.

The main impact of NIS2 on domain name registries is on cybersecurity measures, the handling of registration data and reporting requirements, all of which are subject to fines. Any domain name registry not established in the EU must have a legal representative in the European Union.

Whilst NIS2 covers a very broad subject in general, this document will focus on Article 28 as it is this article that has caused a great deal of debate and uncertainty.

Minimum requirements

It would be particularly valuable if national laws only set minimum requirements that do not go beyond Article 28 and are agnostic to specific technologies and business models in order to limit the risk of market fragmentation. For example, it would be useful if there were no performance requirements, such as pre-validation rather, leaving the choice between pre-validation and post-validation to the companies involved.

For example, some European ccTLDs have strict vetting procedures because of their limited geographical reach. These standards cannot be applied globally. The community needs to work on other mechanisms to ensure that DNS Abuse is responded to as quickly as possible and is ideally prevented.

Allocation of tasks / data minimisation

There are different models used in the domain industry to offer domain name registrations. Not only are ccTLDs operated in a different way from gTLDs, but within these two groups there are also different setups.

For domain name registries, the following constellations come to mind:

- There are registries that have direct contractual relationships with registrants and therefore have all the registration data in their databases.
- There are registries that have eligibility requirements for registrants or nexus requirements that they may need to enforce, so they also receive registration data from registrars.
- Then there are registries that have no direct relationship with the data subject and receive only limited technical data from registrars needed to operate the registry's provisioning and resolution functions. In these cases, registries have no purpose in obtaining and holding registrant data.

When it comes to domain name registrars or resellers, these organisations tend to be very small. This is particularly true for ccTLD registrars and resellers (or resellers of resellers). There are a large number of such entities managing less than 50 domain names.

Article 28 requires Top Level Domain Registries and entities offering the registration of domain names to perform various tasks, which are listed in Art. 28 (1) - (5) – namely, the maintenance of a registration database,

the verification of registration data, the provision of a public WHOIS service and the processing of requests for disclosure.

Art. 28 (6) specifies that there shall be no duplication of collection and that registries and entities providing domain name registration services shall cooperate with each other.

This clause potentially leaves room for an interpretation that all entities involved in a given domain name registration – for example, the registry, the registrar, reseller 1, reseller 2 (sub-reseller) – must perform all tasks except collection. The consequence of this interpretation could lead to multiple databases operated by multiple entities performing the same processing activities – namely, validation of registration data, provision of public WHOIS and handling of disclosure requests.

In many cases, such a requirement would even involve the export of data to entities outside of the EU, notably to the US. The eco association trusts that this is not intended to be the default situation.

We therefore believe that it would be advisable to require only that the processing of the same data be carried out by one body, provided that there are agreements in place between them on the division of tasks. Such agreements would fulfil the legal requirement of cooperation in Art. 28 (6).

By way of illustration, a ccTLD registry with a large number of registrars may choose to perform all of the tasks listed in Art. 28 and include them in its agreements with registrars, while a gTLD registry that has no purpose for processing registry data may choose to have the tasks performed by registrars who have the customer relationship and accordingly cover the allocation of responsibilities in their agreements.

Such an approach would also respect the principle of data minimisation, which would be applied to the fullest extent possible.

Legal entities

A point of contention in the EPDP deliberations at ICANN was how to deal with the data of legal entities. While NIS2 requires operators to publish the data of legal entities, it also points out the caveat that the data of legal entities must not be published if it contains personal data. On this basis, NIS2 would not help operators to achieve legal certainty. Perhaps it would be possible to grant the operators of the public WHOIS service the right to publish legal entity data without risk by removing the burden of checking legal entity data for personal data.

Another difficulty is that the email from the registrant is expected to be made public unless it contains personal information: Machines can't judge whether an address is a natural person or not, so this has to be done manually in the registration process for legal entities. We are of the strong opinion that the message to governments should not go beyond the minimum required by the NIS2 Directive when implementing it at national level.

Legitimate access seekers

Access to information in response to lawful and duly substantiated requests from legitimate access seekers is required by the NIS2 Directive, and domain name registries must respond within 72 hours, which may be difficult to manage. The European Commission can provide guidance on access procedures and should, as far as possible, take into account the standards developed by the multi-stakeholder governance structures. Accuracy and verification procedures are not defined in NIS2, but there is a recital with specific requirements that could become a moving target in the future, depending on implementation.