Submission of ICANN Business Constituency

Fö2024/00496
New Rules on Cybersecurity

Via email:
fo.remissvar@regeringskansliet.se
visnja.raguz@regeringskansliet.se

Thank you for the opportunity to comment on this important matter of cybersecurity.

Introduction

About the ICANN Business Constituency

The Business Constituency (BC) is the voice within ICANN (the Internet Corporation for Assigned Names and Numbers – the coordinating body of DNS policy) of commercial internet users. ICANN is a global body with responsibility for certain policies that relate to the DNS. Domain names are the names consumers and businesses rely upon to find websites for legitimate products and services on the Internet.

Focusing on Article 28

The revised Network and Information Security Directive (NIS2) is a broad, far-reaching directive that comprehensively addresses various areas of focus; however, not all important elements of the directive are included in Sweden's proposal.

A critical element of NIS2 is Article 28 and Recitals 109 to 112, which prescribe the treatment and availability of domain name registration data (known as WHOIS data). WHOIS is an important tool in the fight against the growing problems of cybercrime and abuse via the domain name system (DNS). Lack of reasonable access to this data has helped fuel these difficulties. To maintain a proactive stance against cybercrime, Sweden must ensure the same level of robust implementation of Article 28 as other EU jurisdictions.

Sweden's proposed transposition of Article 28, relative to other EU nations, is comparatively weak and should be broader than the focus on the .SE and .NL top-level domains. A less than vigorous transposition will risk attracting to Sweden's jurisdiction domain name registries and registrars that are irresponsible actors and willingly turn a blind eye to cybercriminals of all kinds that make use of their services.

The European Commission's recently published recommendation on measures to combat counterfeiting further establishes a suitably broad inclusion of factors necessary for Sweden to consider in its transposition.

In this comment, we provide further specific input regarding the effective transposition of Article 28. While this submission is made by the Business Constituency of ICANN, we note that the positions set forth below, including all suggested legislative language, have been reviewed and endorsed with respect to EU Member State implementation of Article 28 by eighteen different organisations and associations devoted to cybersecurity, child safety, medicine and patient safety, anti-counterfeiting and consumer protection, and IP protection. These include the EU Cybercrime Task Force (EUCTF), composed of heads of national cybercrime units from various member states as well as representatives of Europol and the Commission, and the Cybersecurity Tech Accord (CTA). The CTA includes over 150 leading cybersecurity, technology and online commerce companies as signatories (See:

https://cybertechaccord.org/signatories/). The CTA recently published a blog post about these points and suggested legislative language for Member State implementation of Article 28 of the NIS2 Directive, which may be found at this link: https://cybertechaccord.org/eus-network-and-information-system-directive-nis-2-can-restore-access-to-critical-whois-data/

The eighteen orgranisations that have endorsed the positions and suggested legislative language set forth below are as follows:

- **ABAC/BAAN** Belgian Anticounterfeiting Association https://www.abac-baan.com/
- **AIM** European Brands Association https://www.aim.be/
- **ANDEMA** Spanish Anti-Counterfeiting Group https://www.andema.org/en/sobre-andema/sobre-nosotros
- **APM** German Anticounterfeiting Association https://apm.net/
- **APWG** Anti-Phishing Working Group https://apwg.org/
- **ASOP** EU Alliance for Safe Online Pharmacy in the EU https://buysaferx.pharmacy/eu/
- **CHIS** Children's Charities' Coalition on Internet Safety https://www.ecpat.org.uk/childrens-charities-coalition-on-internet-safety-digital-manifesto
- **COMITE COLBERT** The Voice of French Luxury https://www.comitecolbert.com/
- **COA** Coalition for Online Accountability http://www.onlineaccountability.net/
- **CTA** Cybersecurity Tech Accord https://cybertechaccord.org/
- **ECPAT INTERNATIONAL** Ending Sexual Exploitation of Children https://ecpat.org/
- **EUCTF** European Union Cybercrime Task Force https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf
- **REACT** The Anticounterfeiting Network https://www.react.org/
- **RETTIGHEDS ALLIANCEN** Danish Rights Alliance https://rettighedsalliancen.com/
- **RATTIGHETS ALLIANSEN** Swedish Rights Alliance http://www.rattighetsalliansen.com/en/
- **SPAMHAUS** The Spamhaus Project https://www.spamhaus.org/
- **TRACIT** Transnational Alliance to Combat Illicit Trade https://www.tracit.org/
- **UNIFAB** French Association to Promote and Protect Intellectual Property https://www.unifab.com/

NIS2 ARTICLE 28: EU MEMBER STATE IMPLEMENTATION

While the provisions of Article 28 may appear rather technical in nature, robust implementation is essential to the fight against the growing problem of cybercrime. Resolving current problems related to the accuracy and accessibility of registrant data (WHOIS data) is essential for cybersecurity and law enforcement. Requiring the accuracy and verification of such data is not only crucial to the investigation of cybercrime, but also establishes accountability so as to prevent cybercrime in the first place. Rigorous implementation in national law of Article 28's provisions will significantly address the increasing harms that result from anonymous illegal activity that currently goes unchecked by ICANN (the overseer of the DNS), and many registries, registrars and other domain name registration services, including privacy and proxy service providers and resellers. To protect the general public, as well as businesses and organisations harmed by internet wrongdoing, NIS2 is an important opportunity to increase public safety and effectively combat a broad array of criminal activities on the internet.

Significantly, we note that EU Member State law that explicitly sets forth the points described below and set forth in Annex 2 in their implementation of Article 28 will help achieve the objectives set forth in Article 6 of the Second Additional Protocol to the Budapest Cybercrime Convention, which concerns requests for domain name registration information.[1] Such requests will help serve to combat cybercrime only if the registration data delivered in response is accurate, verified and consists of the data of the beneficial user of the domain name, not simply the ineffectual placeholder data of a privacy or proxy service provider.

These recommendations have the support of EU cybercrime law enforcement experts (EUCTF) as well as organisations and associations devoted to cybersecurity, child safety, medicine and patient safety, anti-counterfeiting and consumer protection, and IP protection.

In January 2022, the European Commission Study on Domain Name System (DNS) Abuse stated unequivocally that "[t]he contractual obligations in place for gTLD registries and registrars (and their resellers, if any) have been found **unachieved, ineffective, and/or unenforced** by periodic reviews mandated by ICANN Bylaws"[2] (emphasis added). Therefore, **ICANN contracts and policies cannot be relied upon** to provide detailed substance to the obligations set forth in Article 28. Rather, EU Member States must provide clear and explicit requirements in their transposition of Article 28 and implementation in their national laws.

Indeed, the Commission Study highlighted the best practices of European country code top-level domains (ccTLDs), including .EU, that "contribute to reduce malicious activities on the Internet." By implementing the language suggested below with its specific requirements into national law, EU Member States will assist in bringing generic top-level domains (gTLDs) up to the same level of responsibility that they have already put into practice for their own ccTLDs and for .EU. As a reference, Annex 2 sets forth the existing language of Article 28 of NIS2 with additional language that serves to implement the specific points provided in this paper that will achieve the intended objectives of Article 28 and the overall goal of NIS2 to increase the level of cybersecurity across the Union.

The important aspects of Article 28 that require the most attention with respect to implementation in Member State national law are as follows:

- **LEGITIMATE ACCESS SEEKERS**:
    - **Rationale** - Recital 110 defines "legitimate access seeker(s)" of WHOIS data as set forth in Article 28 paragraph 5 as "any natural or legal person making a request pursuant to Union or national law." National law must therefore clarify that "legitimate access seekers" be defined not only as governmental agencies such as law enforcement, but also any natural or legal person making a request to access WHOIS data to investigate illegality, including without limitation for the establishment, exercise, or defense of cybersecurity, intellectual property, consumer protection, or other legal claims. Indeed, law enforcement agencies often collaborate with and rely upon independent researchers and non-governmental organisations to track and combat illegal online activity.[3]

[1] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224
[2] European Commission Study on Domain Name System Abuse, January 2022 at page 136. The full study is available at: https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1
[3] See for example European Cybercrime Centre, which "aims to engage public and private sector stakeholders whose skills, resources, and reach are needed alongside law enforcement efforts to create a safer digital environment." https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Furthermore, as the Governmental Advisory Committee to ICANN has noted in its consensus advice to the ICANN Board of Directors, "Law enforcement agencies investigations may be compromised if requests for domain registration data are not kept confidential."[4] Yet there is currently no process or requirement for the maintenance of confidentiality of law enforcement access requests. Indeed, some registrars refuse to comply with confidentiality requests from law enforcement agencies for domain name registration data unless those requests are accompanied by a court order requiring confidentiality. Clearly, such refusals hamper law enforcement investigations and provide increasing coverage for cybercriminals. More than 20 years ago the Organisation for Economic Cooperation and Development (OECD) noted how domain name registration data is often a first step for investigation of cybercrimes and stated "Accurate contact data for all domain name registrants across the gTLDs and ccTLDs should be readily available to appropriate consumer protection law enforcement officials."[5] Therefore, Member State law implementing Article 28 should set out clear requirements that: (i) prioritize fulfilling access requests from law enforcement agencies and, (ii) upon request from law enforcement agencies, require that their data access requests and the responses to such requests be kept confidential.

- **Suggested Language for Implementation -** ***"Legitimate access seekers include any natural or legal person making a request for the establishment, exercise, or defense of criminal, civil or other legal claims pursuant to any Union law or any law of [Member State]. TLD name registries and the entities providing domain name registration services shall give priority to fulfilling requests submitted by law enforcement agencies. Furthermore, upon request from a law enforcement agency, TLD name registries and the entities providing domain name registration services must keep confidential the existence of the access request (including whether access to data has been granted in response to such request)."***

- **PRIVACY AND PROXY INFORMATION:**

  - **Rationale** - When a legitimate access request for WHOIS data is made, the underlying data of the actual customer/beneficial user of the domain name must be revealed and not just the data of the privacy or proxy service provider if such a privacy or proxy service was used in the registration process. This requirement must apply irrespective of whether or not the privacy/proxy service used is affiliated with the TLD name registry or registrar. The transposition of Article 28 should clarify that it is the responsibility of the TLD name registry or registrar or reseller to obtain the underlying data of the actual customer/beneficial user to deliver in response to legitimate access requests. Annex 1 attached shows a real-life example of a response from an EU Member State domain registration service provider that *does not* meet this requirement and therefore harms the goals and intentions of the NIS2 Directive. Moreover, a 2021 study by the EUIPO noted that "a significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered via privacy or proxy services" and that since the entry into force of the GDPR the rationale for the legitimate use of privacy or proxy services "has been called into question."[6] Indeed, the TLD name registry for the .NL ccTLD has decided to prohibit the use of privacy/proxy services in all .NL registrations as of October 2023.[7] Clearly, information such as that in the response documented in Annex 1 is not the registration data that the EU co-legislators had in mind as fulfilling the requirement set forth in Recital 110 that "The availability and timely accessibility of domain name registration data to legitimate access seekers is essential for the prevention and combating of DNS abuse, and for the prevention and detection of and response to incidents."

  - **Suggested Language for Implementation** - ***"In providing data in response to legitimate access requests, TLD name registries and the entities providing domain name registration services shall provide the data of the beneficial user of and the point of contact administering the domain name and may not provide***

[4] Governmental Advisory Committee Communique, Cancun, March 2023, p. 11 https://gac.icann.org/advice/communiques/icann76-cancun-communique-es.pdf

[5] OECD (2003-06-02), "Consumer Policy Considerations on the Importance of Accurate and Available WHOIS Data", OECD Digital Economy Papers, No. 73, OECD Publishing, Paris. http://dx.doi.org/10.1787/233072722141

[6] EUIPO "Domain Names: Discussion Paper" March 2021 https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Discussion_Paper_on_Domain_Names/2021_Discussion_Paper_on_Domain_Names_FullR_en.pdf

[7] See https://www.sidn.nl/en/news-and-blogs/privacy-and-proxy-services-prohibited-from-nl-after-1-october#:~:text=From%201%20October%202023%2C%20we,nl%20registrars%20and%20resellers

instead the data of the privacy or proxy registration service provider that may have been used in the domain name registration process."

- **TIMING OF DISCLOSURES:**

  - **Rationale -** Requests by legitimate access seekers for WHOIS data that include personal data must be fulfilled without undue delay. This means that the *disclosures* required by Article 28 must be subjected to specific timelines. Some TLD name registries and registrars assume that Article 28's requirements to "reply without undue delay and in any event within 72 hours of receipt of any requests for access" is satisfied through an automated acknowledgement of receipt, rather than requiring disclosure to legitimate access seekers within 72 hours. Cybercrime, such as ransomware and denial of service attacks, require *immediate* access to WHOIS to investigate and limit such crimes. Furthermore, urgent requests related to serious threats to life, bodily harm, human and child trafficking and other such illegal activities also should be responded to as quickly as possible – in a matter of less than 24 hours, not days.

  - **Suggested Language for Implementation** – ***"Responses to legitimate access requests must provide the requested registration data without undue delay and in any event within 72 hours of receipt of the access request."***

- **ADDRESSING DNS ABUSE AND THE PREVENTION AND DETECTION OF AND RESPONSE TO INCIDENTS AT SCALE:**

  - **Rationale** - For cybersecurity related abuses such as phishing and distribution of malware, cybercriminals will often register dozens and sometimes hundreds or even thousands of domain names over a short period of time. Some registrars offer "bulk registration," which can facilitate the registration of hundreds or thousands of domain names in a matter of minutes. As observed in the Cybercrime Supply Chain Report of 2023, "the domain name system was never intended to supply criminals with thousands of domains in a matter of minutes and do so year after year."[8] Yet the report noted that over 1.5 million domain names associated with cybercrime activity were registered using bulk registration and that bulk registrations accounted for one-third of maliciously registered domain names reported for serving as resources for various cybercrimes. Accordingly, because bulk registration capability has been demonstrated to facilitate cybercrime and appears to significantly outweigh potential legitimate purposes for such processes, the ability to register domain names in bulk should be prohibited.

    In addition, it is critical that legitimate access seekers be able to obtain a list of all of the domain names registered by an entity providing domain name registration services or administered by a TLD name registry that have been registered using the same registrant data. This is often referred to as "reverse WHOIS lookup." As stated in Recital 110, "The availability and timely accessibility of domain name registration data to legitimate access seekers is essential for the prevention and combating of DNS abuse, and for the prevention and detection of and response to incidents." This timely availability and accessibility must include data to satisfy reverse WHOIS lookup requests in order to combat sophisticated and often dispersed cyberattacks and other criminal activity.

  - **Suggested Language for Implementation** – **"*Member States shall prohibit TLD name registries and entities providing domain name registration services from providing or facilitating bulk registration of domain names via algorithms, software, automated protocols or any other similar method. With respect to a domain name associated with abusive or illegal activity that has been alleged by the legitimate access seeker, TLD name registries and entities providing domain name registration services must provide a list of all the domain names that they administer or have registered under the same registrant data if requested by the legitimate access seeker."***

- **PUBLICATION OF DATA OF LEGAL PERSONS:**

  - **Rationale** - The WHOIS data of legal entities (at minimum, name and working/verified telephone number and working/verified contact email address) must be made publicly available per paragraph 4 of Article 28 and Recital 112. ICANN, registries, and registrars for years have incorrectly represented that the GDPR

[8] Cybercrime Supply Chain 2023, p. 4, 34 available at: https://www.m3aawg.org/blog/CybercrimeSupplyChain2023

also applies to information identifying legal entities, rather than only to data of natural persons. This misguided interpretation has resulted in unnecessary restrictions of the entire WHOIS database, going far beyond any need to protect the privacy of individual internet users/registrants, and has led to the WHOIS system going dark and thus caused serious and unwarranted obstructions in cybersecurity investigations.[9]

- **Suggested language for Implementation:** ***"TLD name registries and the entities providing domain name registration services shall make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data, including without limitation the registration data of legal entities. To make public means that TLD name registries and the entities providing domain name registration services shall offer a human readable online portal, interface or tool in addition to any automated look-up technical tools and protocols made available through multi-stakeholder entities that oversee technical standards for the domain name system. No fees or other compensation may be charged and no waiver or limitation of potential legal claims or rights may be required for access to such data made publicly available."***

- **VERIFICATION:**

  - **Rationale** - Pursuant to Article 28 paragraphs 1 and 3, TLD name registries and other "entities providing domain name registration services" must verify the accuracy of WHOIS data. It is essential that these obligations apply to privacy and proxy service providers and domain name resellers as well as to registrars and registries. Article 6 paragraph 22 specifically defines privacy and proxy service providers and domain name resellers, along with registrars, as entities providing domain name registration services. Member State legislation should also clearly define privacy and proxy service providers and resellers (as well as registrars) as "entities providing domain name registration services." In addition, it is important that verification procedures be robust and updated to reflect improvements in technologies and processes. Recital 111 requires that these procedures "prevent and correct inaccurate registration data" and "reflect the best practices used within the industry…and progress made in the field of electronic identification" and should include both "ex ante controls carried out at the time of registration and ex poste controls carried out after the registration." While registries may not be able to verify WHOIS data at the time of registration, since the initial collection of the data is usually by registrars and/or privacy/proxy services, they certainly can and should be obligated to undertake ex poste verification procedures.

  - **Suggested Language for Implementation-** ***"Entities providing domain name registration services, including registrars, privacy services, proxy services and domain name resellers, shall engage in ex ante procedures to verify the accuracy of registration data in each of the contact fields set forth in [Article 28 paragraph 2] before permitting a domain name to resolve. At a minimum, TLD name registries shall engage in ex poste procedures to verify the accuracy of registration data in each of the contact fields set forth in [Article 28 paragraph 2] for the domain names that they administer. In all cases, entities providing domain name registration services and TLD name registries shall employ processes and technologies in verification procedures that reflect current best practices of the domain name industry, including those adopted by ccTLD registries."***

- **MITIGATION FOR INACCURATE DATA:**

  - **Rationale** - If the WHOIS data for a particular domain name is materially false, inaccurate and/or incomplete, or if the domain name has been maliciously registered[10], then that domain name should be frozen and not permitted to resolve until the registrant corrects the WHOIS data so that it is accurate, complete and verified. The TLD name registry and the entity providing domain name registration services

[9] See 2021 joint study of Anti-Phishing Working Group and Messaging, Malware and Mobile Anti-Abuse Working Group, which states, in part: "From our analysis of over 270 survey responses, we find that respondents report that changes to WHOIS access . . . continue to significantly impede cyber applications and forensic investigations and thus cause harm or loss to victims of phishing, malware or other cyber attacks." https://apwg.org/m3aawg_apwg_whois_user_survey_report_2021/

[10] According the European Commission Study on Domain Name System Abuse of January 2022, a **maliciously registered domain name** is defined as "a domain name registered with the malicious intent to carry out harmful or illegal activity." Page 7 of Appendix 1 – Technical Report https://op.europa.eu/en/publication-detail/-/publication/d9804355-7f22-11ec-8c40-01aa75ed71a1

should take the same action with respect to **all domain names** that have been registered under the TLD or using the entity's services with the same materially false, inaccurate and/or incomplete WHOIS data. Recital 111's obligation that "TLD name registries and entities providing domain name registration services should establish policies and procedures…**to prevent and correct inaccurate registration data**, in accordance with Union data protection law" (emphasis added) can only be fulfilled if those policies include consequences for domain names registered with materially false or inaccurate registration data. Thus, domain names registered with materially false, inaccurate or incomplete registration data should not be permitted to resolve and function unless and until the registration data is corrected and validated.

- **Suggested Language for Implementation** – "***If domain name registration data is materially false, inaccurate or incomplete, or if a domain name has been maliciously registered, then the relevant TLD name registry and the entity providing domain name registration services shall prevent the transfer of all of the domain names under its administration that have been registered with such same materially false, inaccurate or incomplete information or have been maliciously registered by that customer, and prevent the domain names from resolving. If the registrant fails to correct the registration data within fifteen (15) calendar days after notice to make it complete and accurate as demonstrated by further verification, then the TLD registry and entity providing domain name registration services shall suspend all of the domain names under its administration that were registered with such false, inaccurate or incomplete registrant data, or that have been maliciously registered by that customer."***

- **THICK WHOIS**:

  - **Rationale** - Pursuant to Article 28 and Recital 109, TLD name registries, in addition to registrars, must maintain independent, accurate, verified and complete registrant databases/WHOIS databases. The single TLD name registry for .com and .net (which accounts for more than half of all total registered domain names globally) has contracts with more than 2,000 registrars globally. For government agencies and other legitimate access seekers to be forced to track down the relevant registrar for a .COM or .NET domain name to pursue a WHOIS data request (a registrar may well be located in a non-cooperative country) completely undermines the goal of increasing cybersecurity and instead serves to provide cover and protection for illegal actors. **Yet, that is the situation today**. It is essential that this registry, as well as all other TLD name registries, maintain a complete, accurate and independent database of WHOIS data for **all** of the domain names it administers (often referred to as "Thick WHOIS") and this database **must include** the data of the beneficial user of the domain name and not simply the data of a privacy or proxy service provider that may have been used in the registration process. This critical requirement will ensure that law enforcement authorities and other legitimate access seekers have a centralized and single source from which to seek complete and accurate data about any domain name administered by the TLD name registry. In addition, some registrars, who bear the clearest obligation of data collection under NIS2, may be bad actors, seeking to raise profits by providing cover for registrants engaged in illegal activity by allowing false WHOIS data to be given for registrations. By explicitly setting forth the following requirements in national law, EU Member States will properly fulfill the cybersecurity goals of Article 28 and will achieve significant declines in the abuse of the domain name system to carry out illegal and harmful activity.[11]

  - **Suggested Language for Implementation:** ***TLD name registries must: (i) maintain an independent, complete and accurate database of WHOIS data for each domain name registered in the TLD name registry, (ii) ensure that such database contains the complete contact data (name, email address and telephone number) for the beneficial user of the domain name and not only the data of a privacy or proxy service provider if such a provider was used in the registration process, (iii) verify the accuracy of the contact data required under Article 28 through ex poste independent data verification and accuracy procedures on the data the TLD name registry receives from registrars and any other entities providing domain name registration services, (iv) ensure that each of their registration services, partners, and entities providing registration services comply with accuracy and verification requirements, and (v)***

[11] See, for example, the European Commission's January 2022 Study on Domain Name System Abuse, pp. 158-159, which quantifies an 85% reduction in malicious websites selling counterfeit goods in the .dk TLD, as a result of the .dk registry's improved data verification practices. https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1

suspend and prevent from resolving any domain name registered in the TLD name registry that was registered with materially false, inaccurate or incomplete WHOIS data, or was maliciously registered.

- **FREE DISCLOSURE**:

  - **Rationale –** The accessibility, publication, and disclosure of data as required under Article 28 must be free of charge to the legitimate access seekers. As set forth in Recital 112 "Member States should ensure that all types of access to personal and non-personal domain name registration data are free of charge." In addition, TLD registries and entities providing domain name registration services must not require legitimate access seekers to give up any rights or potential legal claims in order to access registration data.

  - **Suggested Language for Implementation** – ***"Neither TLD name registries nor entities providing domain name registration services may charge any fees or require any compensation and no waiver or limitation of potential legal claims or rights may be required for responding to access requests and supplying registrant data in response to legitimate access requests."***

CONCLUSION:

Implementation of Article 28 of NIS2 and its related Recitals may well include measures that go beyond the points set forth above. However, to make progress towards the goals of achieving a higher level of cybersecurity across the EU, fulfilling the objectives of the Second Protocol of the Budapest Cybercrime Convention, combating and diminishing online illegal activities of all kinds, and better protecting the general public, **clear and explicit implementation of the points described above in Swedish national law is necessary**. **Annex 2 sets forth suggested implementation language in the context of the existing language of Article 28.**

Further Update: On 19 March 2024 the Commission released its Recommendation on Measures to Combat Counterfeiting and Enhance the Enforcement of Intellectual Property Rights. Articles 14 and 15 recommend that TLD name registries and entities providing domain name registration services follow good practices consistent with those described in this paper and the suggested implementation language set forth in Annex 2. These include: (i) rigorous verification of domain name registration data, (ii) measures to detect incorrect registration data and consequences for failure to correct such data, and (iii) recognizing legitimate access seekers to registration data as any legal or natural person seeking access pursuant to Union or national law, including for the enforcement of intellectual property rights. **The Commission Recommendation provides further support and justification to the suggestions made in this paper concerning Member State implementation of Article 28 of NIS2**. The text of Articles 14 and 15 of the Commission Recommendation are provided in Annex 3.

ANNEX 1

The below was a response provided in August 2023 to an access request made in Germany pursuant to a valid Request of Information ("ROI") in accordance with German law that was submitted to the domain reseller and the German registrar. The response provides only the name of the privacy/proxy service and an array of misleading information. **Importantly, this response provides no real or useful information whatsoever concerning the beneficial user of the domain name**.

Clearly, this is not the type of data fulfillment that the EU co-legislators had in mind when they mandated under Article 28 paragraph 5 that "the entities providing domain name registration services [shall] provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers." When government authorities and other legitimate access seekers are investigating and combating cybercrime, particularly cybersecurity incidents like ransomware and denial of service attacks that are *highly* time sensitive, responses such as the below serve only to help and protect cybercriminals and obstruct the goal of increasing cybersecurity.

Therefore, Member State national law implementing NIS2 must *specifically* require that when a legitimate access request is made to a TLD name registry or an entity providing domain name registration services, it is the responsibility of that TLD name registry or entity providing domain name registration services to respond with the data of the individual or organisation that is the actual/beneficial user of the particular domain name. Responses such as the one below need to be clearly identified as **not** complying with the law. Data for a privacy or proxy service provider, obviously, is an insufficient reply and serves only to frustrate and waste the time of those legitimately seeking the data for combating online abuse and investigating illegal activity.

	Organization	Data Protected
	Name	Data Protected Data Protected
	Firstname	Data
	Lastname	Protected Data Protected
	Street	123 Data Protected
	Zip	98033
	City	Kirkland
	Country	US
	State	WA
	Phone	+1.0000000000
	Fax	+1.0000000000
	E-Mail	noreply@data-protected.net

This was registered via Enom as a reseller of 1 API (Germany)...

ANNEX 2

NIS-2 DIRECTIVE ARTICLE 28

SUGGESTED LANGUAGE ADDITIONS FOR EU MEMBER STATE IMPLEMENTATION

HIGHLIGHTED IN YELLOW

Article 28
Database of domain name registration data

1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall require TLD name registries and entities providing domain name registration services, including registration privacy services, proxy services and domain name resellers, to collect, verify and maintain accurate and complete domain name registration data in a dedicated and independent database with due diligence in accordance with Union data protection law as regards data which are personal data. TLD name registries shall ensure that the dedicated and independent databases that they maintain contain the contact information set forth in paragraph 2 of the beneficial user of the domain name and customer of any privacy or proxy service used in the registration of the domain name. Further, Member States shall prohibit TLD name registries and entities providing domain name registration services from providing or facilitating bulk registration of domain names via algorithms, software, automated protocols or any other similar method.

2. For the purposes of paragraph 1, Member States shall require the database of domain name registration data to contain the necessary information to identify and contact each of the holders of the domain names and the points of contact of the beneficial users administering the domain names under the TLDs, including the customers of any privacy or proxy service used in the registration of the domain names. Such information for every domain name registered in the TLD shall include:

(a) the domain name;

(b) the date of registration;

(c) the registrant's 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.

3. Member States shall require the TLD name registries and the entities providing domain name registration services to have, abide by and enforce policies and procedures, including verification procedures, in place to ensure that the databases referred to in paragraph 1 include accurate, verified and complete information. Member States shall require that such policies and procedures at minimum follow the best practices adopted by European country code TLD name registries and shall require such policies and procedures to be made publicly available.

Such policies and procedures shall at minimum require entities providing domain name registration services to engage in ex ante procedures before permitting a domain name to resolve and require TLD name registries to engage in ex poste procedures to verify the accuracy of all of the information set forth in paragraph 2. If domain name registration data is materially false, inaccurate or incomplete, or if a domain name has been maliciously registered, then the relevant TLD name registry and the entity providing domain name registration services shall prevent the transfer of all of the domain names under its administration that have been registered with such materially false, inaccurate or incomplete information or have been maliciously registered by that customer **and** prevent the domain names from resolving. If the registrant fails to correct the registration data within fifteen (15) calendar days after notice to make it complete and accurate as demonstrated by further verification, then the TLD name registry and entity providing domain name registration services shall suspend all of the domain names under its administration that were registered with such materially false, inaccurate or incomplete registrant data, or that have been maliciously registered.

4. Member States shall require the TLD name registries and the entities providing domain name registration services to make publicly available and free of charge, without undue delay after the registration of a domain name, the domain name registration data which are not personal data, including the registration data of legal persons. To make publicly available means that TLD name registries and entities providing domain name registration services shall offer a human readable online portal interface or tool in

addition to any automated look-up technical tools and protocols made available through the multi-stakeholder entities that oversee technical standards for the domain name system.

5. Member States shall require the TLD name registries and the entities providing domain name registration services to provide access to and disclose specific domain name registration data free of charge upon lawful and duly substantiated 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 and disclose such domain name registration data without undue delay and in any event within 72 hours of receipt of any requests for access from legitimate access seekers. Such disclosed domain name registration data must include the data of the beneficial user and point of contact administering the domain name and may not consist only of the data of a privacy or proxy service provider. TLD name registries and the entities providing domain name registration services shall give priority to fulfilling requests submitted by law enforcement agencies. Furthermore, upon request from a law enforcement agency, TLD name registries and the entities providing domain name registration services must keep confidential the existence of the access request (including whether access to data has been granted in response to such request).With respect to a domain name associated with abusive or illegal activity that has been alleged by the legitimate access seeker, TLD name registries and entities providing domain name registration services must provide a list of all of the domain names that they administer under the same registration data if requested by the legitimate access seeker. Member States shall require policies and procedures with regard to the disclosure of such data to be made publicly available. Legitimate access seekers include any natural or legal person making a request for the investigation, establishment, exercise or defense of criminal, civil or other legal claims pursuant to any Union law or any law of [Member State].

6. Compliance with the obligations laid down in paragraphs 1 to 5 shall not result in a duplication of collecting domain name registration data from the data subject. To that end, Member States shall require TLD name registries and entities providing domain name registration services to cooperate with each other. For the purposes of paragraphs 4 and 5, free of charge means no fees or other compensation may be charged and no waiver or limitation of potential legal claims or rights may be required.

ANNEX 3

ARTICLES 14 AND 15 FROM COMMISSION RECOMMENDATION OF

19 MARCH 2024

Domain names providers: Ensuring the protection of IP rights in the Domain Name System

(14) Top Level Domain ('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:

(a) to provide in their terms and conditions that a finding of IP-infringing activities by the competent authority in relation to a domain name or its usage, may lead to the termination of the registration and/or suspension and deletion of the delegation of the domain name;

(b) to provide registrants during the registration process with links to relevant publicly available and online searchable IP registers to enable registrants to check the domain name for possible conflicts with registered IP rights. In this regard, TLD-name registries established in the EU and/or offering services in the EU are encouraged to cooperate and work with the EUIPO on the basis of voluntary agreements to replicate for the TLDs under their administration the existing information and alert system currently operated by the EUIPO and EURid for EU trade marks and the TLD '.eu' and extending them to also cover registered geographical indications;

(c) 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;

(d) 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.

(15) When access to domain name registration data that is personal data is sought, TLD-name registries and entities providing domain name registration services established in the EU and/or offering services in the EU are encouraged to recognise as legitimate access seekers any natural or legal persons who make a request for a right to information pursuant to Directive 2004/48/EC.