REPORT ON THE GENERAL DATA PROTECTION REGULATION
Call for Evidence
DG JUST, Units C3 and 01

8 February 2024

The ICANN Business Constituency welcomes the opportunity to submit this response to the European Commission's Call for Evidence regarding the periodic evaluation and review of the General Data Protection Regulation (GDPR) under Article 97 of the GDPR. The European Union should be applauded for its thought leadership regarding personal data protection, which has now become the standard by which other national data protection frameworks are measured.

However, as noted by others, there are potential enhancements to the GDPR available to close perceived loopholes so that the spirit of the GDPR can be achieved. This comment is specifically limited to ambiguities in the GDPR that have resulted in the vast majority of generic top-level domain (gTLD) registration data (commonly referred to as WHOIS) being unavailable, and the proposed steps that can be taken to resolve this unintended consequence.

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.

Background

Before May 2018, most domain name registration data associated with gTLDs was publicly and freely available under standard agreements between ICANN and its contracted parties (registrars and registries). The data was available to law enforcement, cybersecurity authorities, intellectual property owners, and others with a stake protecting businesses and consumers from fraudulent activity. Yet, instead of adopting a balanced approach (consistent with GDPR) to accessing domain registration data – approaches adopted by most European country code top-level domain (ccTLD) administrators – ICANN's policies were revised to largely eliminate access to and disclosure of all meaningful gTLD registration data. Effectively, since the implementation of GDPR, registries and registrars have fully redacted nearly the entirety of the WHOIS database, making records all but inaccessible, even to those with legitimate interests. For example, according to the most recent report from brand protection authority Tracer.AI, the company submitted 3,106 well-formed WHOIS requests between January-September 2023. Of those 3,106 requests, a full 70% either received no response at all or were outright denied.

Indeed, even requests made by EU data protection authorities (DPAs) for WHOIS in connection with investigations to protect privacy rights have been denied. In October 2018, the European Council stressed the negative consequences to enforcing the law online and to the rights of individuals by "the current situation where access to the non-public WHOIS for public policy objectives is left at the discretion of registries and registrars" and emphasized the necessity to expedite the development of a unified access model. Yet almost half a decade later, the situation has not improved and arguably has worsened. Clearly, EU institutions and Member States recognize the public interest in maintaining a safe and stable internet and in combating cybercrime and illegal activity online. The WHOIS database was – and still is – a critical tool in either preventing or tracking down such fraudulent online behavior.

The recently revised European Union's Network and Information Security Directive (NIS2) recognizes that top-level-domain (TLD) name registries are essential entities of high criticality, and further specifically provides that:

- Maintaining accurate and complete databases of domain name registration data (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. (Recital 109)

- 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. (Recital 110)

- TLD name registries and entities providing domain name registration services should be required to make publicly available domain name registration data that fall outside the scope of Union data protection law, such as data that concern legal persons—making publicly available at least the name of the registrant and the contact telephone number, and the contact email address provided that it does not contain any personal data, such as in the case of email aliases or functional accounts. (Recital 112)

- TLD name registries and entities providing domain name registration services should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should require TLD name registries and entities providing domain name registration services to respond without undue delay to requests for the disclosure of domain name registration data from legitimate access seekers. (Recital 112)

While the NIS2 Directive has addressed some of these gTLD policy deficiencies, Recital 14 of NIS2 also states that "Union data protection law and Union privacy law applies to any processing of personal data under this Directive." We believe, therefore, that additional clarifications are needed to align the NIS2 requirements with GDPR, as described below.

Online crime has increased since the darkening of WHOIS

Criminal activity trend lines suggest that internet-based harms – already unfortunately rampant – have increased since May 2018. These harms now include fraud, intellectual property infringement, distribution of malware, phishing, distribution of child sexual abuse material (CSAM), and distribution of falsified medicines, to name only a few.

The rate of increase in criminal activity is well documented (online misconduct is one of the fastest-growing areas of crime, and costs businesses and their users billions annually). For example, in the area of phishing alone:

In its August 2023 study on phishing trends, the US-based consultant Interisle Consulting Group found[1] that:

- The number of phishing attacks worldwide tripled since May 2020 and continues to trend upward;
- More than one million unique domain names were reported for phishing between May 2022 and April 2023 alone, the most observed by Interisle in any period since May 2020; and
- Two thirds of domain names reported for phishing were maliciously registered, meaning they were intentionally registered by a criminal with the intent of launching a phishing attack.

These trends, unfortunately, show no sign of abating. Industry efforts to curb these types of abuses have proven insufficient.

Our conclusion – and that of many others with expertise in DNS policy – is that the unavailability of WHOIS data presents significant challenges to online enforcement and harm prevention efforts. Meanwhile, bad actors continue to proliferate under the new privacy rules, *harming the very consumers the privacy laws were intended to protect*.

Proposed Enhancements

The BC specifically requests consideration of the following:

- As data accuracy is fundamental principle of data processing under GDPR (see Recital 38), the ability of third parties who rely on authoritative databases to invoke GDPR to notify controllers about and compel correction to inaccuracies would greatly improve the outcome of Article 5. For example, the authoritative WHOIS database, relied upon globally for the safe operation of the internet, should not be filled with inaccurate data and corrected only once the data subject finds that the data contained in such an important database is incorrect.
- Clarification that GDPR Article 6(1)e applies to the collection, maintenance and disclosure of the registration directory databases required under Article 28 of NIS2, since they are necessary for the performance of a task carried out in the public interest, even where government actors are not directly responsible for maintaining such a database or EU or member state law does not enumerate specific requirements for processing.
- Clarification of GDPR Article 6, to ensure that disclosure of domain registration data for the purpose of establishment, exercise or defence of legal claims is considered a lawful basis of processing, consistent with Article 49(e).

Conclusion

We respectfully submit that while GDPR has many lasting good effects, its impact on WHOIS, overall, has been detrimental to the safety and integrity of the BC and those we represent and advocate for, due primarily to the perceived limitations of GDPR as interpreted by ICANN. The unfortunate result is that bad actors are now free to conduct their harmful operations anonymously and without detection.

We therefore urge European authorities to carefully consider the consequences of an impenetrable WHOIS database and consider the potential refinement of critical areas of GDPR as described above.

Thank you for the opportunity to provide our perspective on this important matter.

[1] https://interisle.net/PhishingLandscape2023.html