Comments of the ICANN Business Constituency
on
Article 29 Working Party 11-Apr-2018 Guidance Letter

20-Apr-2018

We write in response to the recent guidance provided by the Article 29 Working Party (WP29) on WHOIS directory compliance with the GDPR. The WP29 guidance reinforces several of our positions on the lawfulness of maintaining public access to certain WHOIS data and the need for a comprehensive, consensus-driven code of conduct or certification for GDPR compliance. We support an individual's right to privacy and are committed to the proper implementation of the GDPR. Now that ICANN has received WP29's guidance, we are writing to provide advice and clarifications on how to implement that advice.

As a preliminary matter, we do not read WP29's letter as a rebuttal of ICANN's position that the GDPR allows for certain WHOIS data to be accessible by the public. WP29's guidance welcomes ICANN's proposed interim model and accreditation program, and largely offers areas for improvement upon the proposed interim model. Given that this model is still in draft form and being negotiated, much of WP29's feedback can be addressed in the final product (e.g., ensuring there is an adequate safeguard for transfers of WHOIS data to third countries, justifying why WHOIS data should be retained for two years, and providing more detail on the purpose for WHOIS data processing and the relationship between these purposes and ICANN's stated legal bases for processing). One message that should be taken from this letter is the need for ICANN Org to become more actively engaged in finalizing and implementing the accreditation and access model currently being developed by the community.

ICANN and its stakeholders have written extensively on the purpose of WHOIS data processing and provided examples of its real-world applications, as well as discussed the reasons for making WHOIS data accessible by the public, the importance of securing this data, and means for protecting WHOIS data subject identities. Moreover, the European Commission reinforced many of these positions in its January 2018 letter to ICANN regarding the GDPR's applicability to WHOIS, while recognizing the need to "preserve the proper use of WHOIS."[1] These positions can easily be incorporated into the final compliance model to satisfy many of the concerns flagged in WP29's guidance.[2]

- ***The GDPR does not restrict consideration of third party purposes when determining the purposes for data processing.***

We recognize WP29's recommendation that ICANN provide more detail on certain purposes outlined in the proposed interim model, and that "purposes pursued by other interested third parties should not determine the purposes pursued by ICANN." Here, it is important to note that the GDPR does not prohibit controllers from considering third parties' needs when determining the purposes for certain data processing. On the contrary, some provisions of the law suggest third party purposes should be considered in certain circumstances. Consider, for example, that one of the six lawful bases for processing personal data under the GDPR is "necessary for the purposes of the legitimate interests

[1] See page 2 of the letter.

[2] ICANN is unique in that it was designed to serve the interests of various stakeholders—registrars and registries, but also law enforcement, businesses, individual rights holders, government agencies, and other stakeholders who use WHOIS services for legitimate purposes. It is therefore critical that ICANN and its stakeholders have the opportunity to design a model that offers a lawful and practical GDPR compliance mechanism.

pursued by the controller *or by a third party*."[3] Several entities subject to the GDPR process data partially or sometimes exclusively to serve a third party's purpose; email marketing providers, social media aggregators, market research and professional services firms are just a few examples.

There are also public policy reasons for allowing ICANN's purpose specifications to reflect the needs of third parties that use WHOIS. For one, these third parties are often exercising or assisting other parties in exercising their rights under EU law. Any GDPR compliance analysis must be done with the broader EU law framework in mind, particularly the Charter of Fundamental Rights. Recital 4 of the GDPR expressly states that the right to the protection of personal data is "not absolute" and "it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality." These fundamental rights include the right to freedom of expression and information and the freedom to conduct a business and states that intellectual property shall be protected—all of which are directly related to the primary purpose of WHOIS data processing: proof and notice of ownership.[4] It is entirely acceptable under the GDPR and public policy that this purpose may reflect or support third party purposes.

Further, the European Commission considers a variety of third party purposes to be valid for WHOIS data processing. The Commission recognizes that WHOIS is used by numerous stakeholders for lawful purposes, including "help in countering intellectual property infringements, finding the source of cyber-attacks or assistance to law enforcement investigations."[5] For this reason, it encouraged ICANN to find a resolution that conforms with the requirements of the GDPR, "in keeping with the objective of maintaining access to WHOIS to the greatest extent possible."[6]

ICANN's Governmental Advisory Committee (GAC) reiterated this position in its March 2018 Communique. In fact, GAC believes ICANN's interim model may restrict maintenance of the current WHOIS system beyond what is required by law. The GAC rightly pointed out that the GDPR provides for "mechanisms to balance various legitimate public and private interests at stake" and that the legitimate interests reflected in ICANN's Bylaws are consistent with those in the GDPR that weigh in favor of allowing data processing, such as "preventing fraud" and "ensuring network and information security," including the ability to resist "unlawful or malicious actions."[7] Indeed, ICANN should consider how these third party uses of WHOIS data directly contribute to ICANN's mission and mandate "to coordinate the stable operation of the Internet's unique identifier systems".

In that vein, Article 154 directs that the "principle of public access to official documents be taken into account when applying [the] Regulation", since "public access to official documents may be considered to be in the public interest". Although WHOIS data is not held by a public body but rather uniquely, through ICANN-accredited registrars, the WHOIS database nevertheless fulfills a comparable purpose, namely allowing public access to the official record of domain name registration details, in very much the same manner as public corporate registries and public trademark databases fulfill a crucial and

---

[3] See GDPR, Art. 6(1)(f) (emphasis added).

[4] See e.g., Department of Commerce, *Improvement of Technical Management of Internet Names and Addresses; Proposed Rule*, at 8829, (Feb. 20, 1998). This purpose was established almost two decades ago at ICANN's inception; the registry was described as a tool for simplifying resolution of disputes over domain name ownership. The agency addressed the need for a public domain registry as it related to trademark disputes, stating "the job of policing trademarks could be considerably easier if domain name databases were readily searchable through a common interface to determine what names are registered, who holds those domain names, and how to contact a domain name holder."

[5] See page 1 of its letter to ICANN.

[6] See page 5 of its technical input on proposed WHOIS models.

[7] See page 9 of the Communique.

legitimate purpose in the public interest. As noted by Article 16 of Directive 2003/98/EC, "Making public all generally available documents held by the public sector — concerning not only the political process but also the legal and administrative process — is a fundamental instrument for extending the right to knowledge, which is a basic principle of democracy. This objective is applicable to institutions at every level, be it local, national or international." Indeed, given that several public registers around Europe will continue to publish personal data online, such as land registries, company registries and registries of IP rights, there are clearly circumstances where transparency is valued over individual anonymity when data relates to actions in the public sphere.[8] The legal basis of such registers is different (article 6e – public task - rather than 6f – legitimate interests), however the justifications are similar and open DNS registries are effectively performing public tasks. Had the internet and DNS developed outside of the multi-stakeholder model there might well have been a statutory basis or international treaty covering these tasks. Accordingly, public access to WHOIS data for legitimate purposes should be viewed within this context and that the same principles should apply as with other "public" data.

- ***Automated port 43 requests are not "bulk transfers" of WHOIS data, and are acceptable under the GDPR, provided they are lawfully completed and necessary to fulfill the purpose of the data processing***

In its discussion of access to non-public WHOIS data, WP29 encourages ICANN to limit access to WHOIS data to minimize risks of unauthorized access and use, including "by enabling access on the basis of search queries only as opposed to bulk transfers." However, automated WHOIS data access via port 43 is *not* a bulk transfer. Port 43 enables a computer-to-computer query for a single, fully-described domain name. Each Port 43 query is subject to applicable access controls, and returns WHOIS data for just the single domain name requested. For example, law enforcement and cybersecurity professionals often do Port 43 WHOIS queries for multiple domain names in order to assess multiple domains for criminal investigations. There may be multiple single-name queries, but these are not requests for "bulk transfers" of WHOIS data.

Additionally, the GDPR generally does not limit the level of access to data that is lawfully processed under the regulation. Assuming those who need access to WHOIS data have a lawful basis for processing the data they request and meet the GDPR's other requirements for processing personal data, they should not be restricted to partial or segmented access. The GDPR treats disclosure of WHOIS data as it would any other disclosure of data; it is allowed if the controller (which would be registrars or registries in this case) has a lawful basis for disclosing the data and complies with the broader requirements in the law, including putting appropriate safeguards in place if the recipient is in a third country that does not ensure an adequate level of data protection[9]. If these standards are met, there are generally no

[8] EURID will continue to publish email address for natural persons under its revised WHOIS policy for GDPR for example, and sets out non-public data may be disclosed to third parties under specified circumstances.

[9] See GDPR, Art. 46(1). Recipients in countries not deemed by the Commission to provide adequate data protection—this includes any WHOIS data recipient in the United States and many other countries—generally can only receive data from a registrar or registry if the registrar or registry has provided "appropriate safeguards" for the data transfer and there are enforceable data subject rights and effective legal remedies. Codes of conduct and certifications approved by the European Commission pursuant to Article 40 or 42 of the GDPR are "appropriate safeguards" if combined with the recipient's binding and enforceable commitment to apply the appropriate safeguard. In the absence of an adequacy decision or of appropriate safeguards, WHOIS data may still be transferred to many of the recipients at issue in the WHOIS context (cybersecurity and operational security investigators, intellectual property holders, and non-governmental public safety and health organizations) for several reasons including: the transfer is necessary for important reasons of public interest recognized in Union or

restrictions on how much WHOIS data recipients can access, nor are there special requirements for these data transfers. [10] It should also be noted that the European Commission has addressed the legality of these transfers and "the need to preserve WHOIS functionality and access to its information" in its statements on the issue.

We urge ICANN to raise the above points in its future discussions with WP29, along with other points now raised by the European Commission and ICANN's own Governmental Advisory Committee, Intellectual Property Constituency, and the At-Large Advisory Committee, to maintain WHOIS to the fullest extent possible and to mandate an access mechanism to non-public WHOIS data.

We look forward to continuing to work with ICANN to identify a practical solution to GDPR compliance for WHOIS directories.

The ICANN Business Constituency

--

This comment was drafted by Margie Milam and Mason Cole, with edits by Paul Mitchell, Steve DelBianco, Tim Chen, Alex Deacon, and Zak Muscovitch

Member State law (Art. 49(1)(d)); the transfer is necessary for the establishment, exercise or defense of legal claims (Art. 49(1)(e)); and the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent (Art. 49(1)(f)).

[10] We recognize that Article 49(1)(g) may limit the amount of data a recipient can access in some cases, however, the recipients at issue in the WHOIS context (cybersecurity and operational security investigators, intellectual property holders, and non-governmental public safety and health organizations) would not need this provision to lawfully receive WHOIS data.