



Brussels, 29 January 2018
Ares(2018)579818

Göran Marby
CEO & President
Internet Corporation for Assigned
Names and Numbers (ICANN)

Dear Mr Marby,

I am writing to you in the context of the Commission's ongoing dialogue with ICANN on the WHOIS system and more particularly on the two objectives how to ensure quick access to its directories for public interest purposes whilst being in full compliance with the EU data protection rules. Compliance of the WHOIS system with EU's data protection rules has been discussed, including with our Member States data protection supervisory authorities, at least since the year 2003 under the current legislation. The upcoming application of the General Data Protection Regulation (GDPR)¹ on 25 May 2018 provides an opportunity to now address the issue and implement a pragmatic and workable solution for the future.

The Commission is well aware that the WHOIS system is currently used by a variety of stakeholders for different purposes, including for achieving public policy objectives (e.g. through identification of contact points for network operators and administrators, help in countering intellectual property infringements, finding the source of cyber-attacks or assistance to law enforcement investigations), as already set out in the ICANN Governmental Advisory Committee's 2007 WHOIS Principles². This reflects the broad general interest missions fulfilled by the Domain Name System and by ICANN as the organisation managing this key resource, in the framework of a multistakeholder process which the Commission supports.

We would like to underline the importance of these objectives and the corresponding need to preserve WHOIS functionality and access to its information. The EU Member States have also stressed the importance of "ensuring swiftly accessible and accurate WHOIS databases of IP-addresses and domain names, so that law enforcement capabilities and public interests are safeguarded."³ In this respect, EU law enforcement authorities and individual investigation units have

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.

² https://gacweb.icann.org/download/attachments/28278834/WHOIS_principles.pdf.

³ Council Conclusions of 20 November 2017 on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 14435/17.

informed the Commission that a WHOIS lookup is the first step in many cases involving abuse of networked resources and that they make a significant number of lookups per week.

At the same time, there is a need to comply with the GDPR. This is important not just to ensure respect for the fundamental right to personal data protection, but also for the stability, robustness and accuracy of the WHOIS system as an integral part of the infrastructure that allows the global interoperability of Internet services.

In this context, the Commission welcomes the ongoing efforts of ICANN and the multistakeholder community to clarify the technical and legal requirements and develop data processing models that preserve the proper use of WHOIS while ensuring full compliance with the (current and future) EU data protection rules. The Commission takes note of ICANN's recent commitment "to ensure compliance with the GDPR while maintaining WHOIS to the greatest extent possible"⁴, as well as of the recent publication for discussion within the ICANN community of three proposed models for collecting registration data and implementing registration directory services. We appreciate the complexity of this process and reiterate our commitment to actively engage in the discussions with you and the community of WHOIS stakeholders, in particular when looking at the three proposed models.

The GDPR rests on the same core principles as the current data protection rules that have been in place in the EU and our Member States for many years. These include the following principles that, at first sight, would seem to be most relevant for the WHOIS system, in particular:

- the concept of **personal data** which determines the applicability of the EU data protection rules (Articles 1(1), 4(1) of the GDPR);
- the principle of **purpose limitation** which requires that personal data must only be processed for a specified, explicit and legitimate purpose (Article 5(1)(b) of the GDPR);
- the principle of **lawful processing** which requires that the processing of personal data has a proper legal basis (Article 5(1)(a) of the GDPR); in the case of the operation of the WHOIS system, legal bases such as, for instance, the necessity of the processing for the performance of a contract or a task carried out in the public interest⁵, or the legitimate interests of the controller (Article 6(1)(b), (e) and (f) of the GDPR) could be considered;
- the principle of **data minimisation**, according to which the personal data processed must be adequate, relevant and limited to what is necessary in relation to the purposes of processing (Article 5(1)(c) of the GDPR);
- the principle of **data accuracy** which requires that the data must be accurate and, where necessary, kept up to date (and that every reasonable step is taken to ensure that personal data that is inaccurate is erased or rectified without delay) (Article 5(1)(d) of the GDPR);

⁴ <https://www.icann.org/news/blog/data-protection-and-privacy-update-plans-for-the-new-year>

⁵ Such public interests include, for instance, ensuring cybersecurity and the stability of the Internet, preventing and fighting crime, protecting intellectual property and copyright, or enforcing consumer protection measures.

- the principle of **limited data retention**, according to which data may only be kept in a form which permits identification of individual data subjects for no longer than is necessary for the purposes for which it is processed (Article 5(1)(e) of the GDPR).

I would like to stress that these principles are shared by many countries around the world as they form an integral part of any modern data protection framework. Moreover, EU data protection rules are not different from other types of regulatory requirements that stakeholders involved in the WHOIS system have to follow in the EU or elsewhere.

Compared to the current EU data protection acquis, the GDPR does not create additional burdens for business operators (such as registries and registrars) and in fact facilitates compliance as it ensures harmonisation in terms of rules and their application. It also offers new tools allowing business involvement in drawing up data protection-compliant systems specifically designed for a particular type of data processing activity (such as the DNS-WHOIS system might represent). This includes, for instance, approved codes of conduct (Articles 40, 41 of the GDPR) which can help to demonstrate compliance with EU data protection law. Last but not least, these rules are flexible. Rather than offering "binary" solutions whereby data processing operations such as access to the WHOIS system are either allowed or prohibited, data controllers and processors can work within this framework to develop pragmatic solutions, for instance by trying to differentiate between those categories of data that can be made public from those which cannot.

I understand that this is exactly the type of analysis that ICANN, together with its stakeholder community, is currently carrying out. In its recent letter addressed to ICANN the Article 29 Working Party again invites ICANN and its stakeholders to enter into a dialogue to discuss data protection issues affecting the WHOIS system, including on possible ways to successfully address them. As competent authorities for enforcing compliance with the EU data protection legal framework, working in close cooperation with data protection authorities is crucial and will help to ensure that a stable solution providing legal certainty can be found.

In identifying solutions that meet these requirements, ICANN should consider the following points:

As the GDPR only applies to personal data of natural persons, in a first step, a distinction should be made between data that fall within the scope of the GDPR and other data elements.

Second, to ensure transparency and fairness in the processing of WHOIS data, it is of utmost importance that ICANN clearly specifies the different purposes for processing, including the pursuit of certain public policy objectives in the legitimate interest of the controller or third parties, and that data subjects, in particular registrants, are provided with this information and other relevant information about the data processing in a clear form at the moment of collecting the registration data. Registrars should be given certainty on what data they have to collect and for which of these purposes, in keeping with the aim to maintain the WHOIS to the fullest extent possible.

Third, as regards access to specific data elements falling within the scope of application of the GDPR, careful consideration needs to be given to the extent to which access to specific categories of data may continue to be public and unrestricted, or whether some restriction should be introduced to ensure that the accessible information is relevant and limited to what is necessary in relation to the different purposes of processing. Where specific measures to ensure the protection of personal data,

of which gated access is but one option, are considered necessary, the practical needs for law enforcement authorities' investigations should be duly taken into consideration and clear and workable access procedures should be put in place that meet the needs of law enforcement authorities in particular with respect to high volumes of requests and swiftness of access. Specifically, it would be important for these authorities for the new model to maintain, to the extent possible, while ensuring full compliance with the GDPR requirements, a functionally centralised way to access to relevant data. The power of such authorities to access data through that centralised system would remain determined by national law.

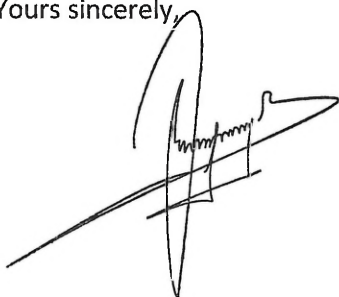
Fourth, in creating such a system, the implementation of safeguards against abuse should be considered to ensure a level of security appropriate to the risk. This could for example consist in a limitation of the number of records that can be accessed per a given time period, as appropriate in view of the legitimate use. The practical needs for law enforcement authorities' investigations should be duly taken into consideration in this respect as well.

Fifth, if a system based on accreditation of users is considered, then the mechanism for accreditation and subsequent access has to respect and ensure both the confidentiality of communication as well as law enforcement authorities' investigations.

Finally, as far as specific requirements for access by law enforcement to WHOIS data are concerned, I would like to stress that these are laid down by national criminal law, which authorities are bound to respect. The specific requirements are not regulated by the GDPR itself, but by other legal instruments and may differ from EU Member State to Member State (e.g. ex-post validation by judicial authorities or need to obtain a court order).

The Commission reiterates its offer to support the efforts of ICANN and its stakeholders to facilitate exchanges with the EU data protection authorities, as appropriate. The Commission published further guidance on the General Data Protection Regulation, including through a set of "Questions & Answers" for both citizens and business operators, on 24 January 2018.

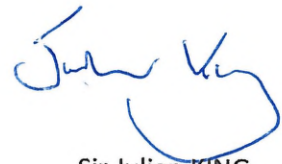
Yours sincerely,



Dimitris AVRAMOPOULOS
Commissioner for Migration,
Home Affairs and Citizenship



Věra JOUROVA
Commissioner for Justice,
Consumers and Gender Equality



Sir Julian KING
Commissioner for
the Security Union

CC: First Vice-President Frans Timmermans
Vice-President Andrus Ansip
Commissioner Mariya Gabriel