

ARTICLE 29 Data Protection Working Party



Brussels, 26 September 2012

Dr. Steve Crocker and Mr. Akram Atallah
Chairman and interim CEO of the Board of
Directors
Internet Corporation for Assigned
Names and Numbers (ICANN)
4676 Admiralty Way, Suite 330
Marina del Rey, CA 90292-6601

By email to the Director of Board Support:
diane.schroeder@icann.org

Subject: Comments on the data protection impact of the revision of the ICANN RAA concerning accuracy and data retention of WHOIS data

Dear Mr Crocker and Mr Atallah,

In the context of ICANN's revision of the Registrar Accreditation Agreement (RAA) and the RAA Negotiations Summary Memo¹, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Article 29 WP)² wishes to respond to your call for input from data protection authorities.³

The Working Party limits this contribution to proposed changes in the RAA that will likely affect the personal data protection rights of European citizens that have registered or will register a domain name.

¹ RAA Negotiations Summary Memo, ICANN Proposed DRAFT 4 June 2012, URL: <http://prague44.icann.org/meetings/prague2012/presentation-raa-negotiation-issues-04jun12-en.pdf>

² The Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data is an independent advisory body on data protection and privacy, set up under Article 29 of the Data Protection Directive 95/46/EC. The Article 29 Working Party is competent to examine any question covering the application of the data protection directives in order to contribute to the uniform application of the directives. It carries out this task by issuing recommendations, opinions and working documents.

³ Can authorities expert in data privacy assist in proposing how ICANN and the Registrars should address the competing legal regimens into a standard that can be uniformly implemented? RAA Negotiations Summary Memo, p. 5.

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO59 2/13.

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm

The Working Party recalls its previous contributions to the process of collecting and disclosing WHOIS data, as included in the Opinion 2/2003 on the application of the data protection principles to WHOIS directories⁴ as well as its letters of 22 June 2006 to the Board of Directors of ICANN⁵ and of 12 March 2007 to the Chairman of the Board of Directors of ICANN⁶ in which the relevant data protection principles have been outlined.

The Working Party notes that the proposed new RAA contains two new requirements for *registrars*, the private corporations that offer internet domain names to the public and that are responsible for maintaining the contact details of domain name holders in the publicly accessible WHOIS database.

1. Annual re-verification of contact details

The first issue is a new requirement for registrars to verify domain name holders' contact details via telephone and e-mail, and to annually re-verify these contact details. The proposed *Whois accuracy program specification*⁷ makes it mandatory for registrars to obtain and verify both an e-mail address and a telephone number from all domain name holders and to annually re-verify these details, by either calling or sending an e-mail or SMS with a unique code that has to be verified by the registrant.

Accuracy of personal data is an important requirement in data protection law. However, the necessity to keep personal data accurate may not lead to an excessive collection or further processing of personal data. It is important to distinguish between contact details collected by registrars in the course of a contract, and contact details that have to be published in the WHOIS database.

The problem of inaccurate contact details in the WHOIS database cannot be solved without addressing the root of the problem: **the unlimited public accessibility of private contact details in the WHOIS database**. It is a fact that these contact details are being harvested on a large scale and abused for spamming. **In other words, the way the system is designed provides a strong incentive for natural persons to provide inaccurate contact details. Regrettably, ICANN has decided not to work on alternative layered access models, such as the OPoC model repeatedly proposed as proportionate alternative by the Working Party.**

As highlighted in previous letters to ICANN, purpose limitation/finality is crucial to determine whether the processing of personal data is compliant with the provisions of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("the Data Protection Directive"), as translated in the national laws of the 27 EU Member States. As you explicitly acknowledge in the Negotiations Summary, the request for annual re-verification of domain name holders data as well as the request to verify both the e-mail address as well as the telephone number, originates from law enforcement.

⁴ URL: <http://www.icann.org/correspondence/schaar-to-cerf-22jun06.pdf>

⁵ URL: <http://gns0.icann.org/correspondence/schaar-to-cerf-12mar07.pdf>

⁶ Whois accuracy program specification, ICANN Proposed DRAFT 3 June 2012, IRI- 39306v3 1, URL: <http://prague44.icann.org/meetings/prague2012/presentation-whois-accuracy-03jun12-en.pdf>

⁷ URL: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp76_en.pdf

In assessing these proposals, ICANN should be aware that the purpose of collecting and publishing contact details in the WHOIS database is to facilitate contact about technical issues. The original purpose definition reads: *"The purpose of the gTLD Whois service is to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS nameserver."*

In your summary of the debate about (public accessibility of) WHOIS DATA you write: *"Over time, WHOIS data has been increasingly used for other constructive and beneficial purposes; (...) However, some WHOIS data uses that have emerged are viewed as potentially negative;(...)."*⁸

The fact that WHOIS data can be used for other beneficial purposes does not in itself legitimise the collection and processing of personal data for those other purposes.

The Working Party finds the proposed new requirement to annually re-verify both the telephone number and the e-mail address and publish these contact details in the publicly accessible WHOIS database excessive and therefore unlawful. Because ICANN is not addressing the root of the problem, the proposed solution is a disproportionate infringement of the right to protection of personal data.

2. Data retention

The second issue is a new requirement for registrars to retain data of domain name holders for a period of two years after the contract for the domain has been ended.

The proposed Data retention specification⁹ has a very broad scope. It is not limited to the personal data collected for the WHOIS database, but also specifies other categories of data that can be processed by registrars, such as telephone numbers and e-mail addresses not contained in the WHOIS data as well as credit card data (*means and source of payment or a transaction number provided by a third party payment processor*), communication identifiers such as a Skype handle and log files containing the source IP address and HTTP headers, dates, times, and time zones of communications and sessions, including initial registration.

This proposed new requirement does not stem from any legal requirement in Europe¹⁰, but again, is explicitly introduced by ICANN to accommodate wishes from law enforcement.

The Working Party strongly objects to the introduction of data retention by means of a contract issued by a private corporation in order to facilitate (public) law enforcement. If there is a pressing social need for specific collections of personal data to be available for law enforcement, and the proposed data retention is proportionate to the legitimate aim pursued, it

⁸ URL: <http://www.icann.org/en/resources/policy/background/whois>

⁹ Data retention specification, ICANN Proposed DRAFT 3 June 2012, IRI--33673v4, URL:

<http://prague44.icann.org/meetings/prague2012/presentation-data-retention-03jun12-en.pdf>

¹⁰ The European data retention directive 2006/24/EC imposes data retention obligations on providers of public electronic communication networks and services. Registrars are not such providers and are therefore not subjected to this European data retention obligation.

is up to national governments to introduce legislation that meets the demands of article 8 of the European Convention on Human Rights and article 17 of the International Covenant on Civil and Political rights.¹¹

The fact that these personal data can be useful for law enforcement does not legitimise the retention of these personal data after termination of the contract. In fact, such a retention period would undermine the first new requirement, to re-verify the contact details every year. If ICANN would be able to prove the necessity for such a yearly re-verification for the purpose of facilitating technical contact with domain name holders, any data kept beyond one year would in fact be excessive, because apparently to a large extent outdated or otherwise unreliable.

Because there is no legitimate purpose, and in connection with that, no legal ground for the data processing, the proposed data retention requirement is unlawful in Europe. Since the registrars (both within Europe and worldwide to the extent they are processing personal data from EU citizens) are data controllers (responsible for the collection and processing of personal data), the Working Party is concerned that this new obligation will put them in the uncomfortable position of violating European data protection law. The Working Party would deeply regret a situation where data protection authorities were to be forced to enforce compliance and urges you to rethink the proposals.

The Working Party has on several occasions expressed an interest in being consulted by ICANN about privacy-related WHOIS issues.¹² We repeat that we are ready to discuss any issue that ICANN feels would be useful in relation to the application of EU and national data protection legislation in respect of WHOIS services and would appreciate it if the relevant ICANN staff would contact the Working Party to ensure that ICANN has a full understanding of the concerns we have expressed.

Yours sincerely,

On behalf of the Article 29 Working Party,

Jacob Kohnstamm
Chairman of the Article 29
Working Party

¹¹ Obligations with regard to the protection of personal data also follow from the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) and the UN Guidelines concerning computerized personal data files (1990).

¹² See also the letter from the WP29 Chairman of 24 October 2007, URL: <http://gnso.icann.org/correspondence/cerf-to-schaar-24oct07.pdf>