**LETTER**

**To:** Neelie Kroes, European Commissioner for Digital Agenda, Vice-President of the European Commission
**From:** eLabEurope
HEC-NYU Regulatory Policy Clinic
**Re:** European Commission position on internet governance reform : Taking into account the need for compliance of ICANN to EU data protection laws

---

Dear Commissioner,

**Today, the internet governing body's decisions question important aspects of the EU data protection legal scheme. Unless the European Commission takes a clear and firm stance now, this state of fact might quickly become more threatening.**

The ongoing reform of the Internet governance provides the right and only opportunity for the EU to have its say on the global scene and to defend the fundamental rights of its citizens, as protected by our legal framework.

In the light of the intentions already expressed, we hope that the EU will now strongly weigh in the international negotiations and have its voice heard. Indeed, on February, 12th 2014, the European Commission stated that "Europe must contribute to a credible way forward for global internet governance. Europe must play a strong role in defining what the net of the future looks like."

The European Commission roadmap to NETMundial, on April, 23-24 2014, added that "The Commission proposes to convene, together with interested parties, a series of workshops with international experts in law, ethics, social sciences, economics, international relations and technology, in order to develop concrete and actionable recommendations to ensure coherence between existing normative frameworks and new forms of Internet-enabled norm-setting. (…) The European Commission plans to launch an in-depth review of the risks, at international level, of conflicts of laws and jurisdictions arising on the Internet and assess all mechanisms, processes and tools available and necessary to solve such conflicts."

**We at eLabEurope, as a newly founded civic organization, have a strong interest in the development of data protection laws governing the rights of the European citizens.** For several weeks, we have received input from members of the public with regards to data retention and protection, through our massive open online course (MOOC) on Coursera, entitled "Understanding Europe, why it matters and what it can offer you". Through this letter, we hope to express the European public interest, and we hope that we can collaborate together in addressing some of the challenges brought about by the governance of internet.

**We would be grateful if you could take into account - in the position of the European Commission on Internet Corporation for Assigned Names and Numbers (ICANN) reform - the data protection violations that we demonstrate having being**

**committed by ICANN's 2013 Registrar Accreditation Agreement (RAA) in breach of the EU legal framework.**

We indeed believe that the 2013 RAA is in direct violation of European Union Law, specifically of the Data Protection Directive (Directive 95/46/EC). The 2013 RAA impinges on the fundamental human rights granted to the citizens of the European Union in the protection and retention of personal data.

We believe that there needs to be a remedy for such violations, and that the European Commission, as watchdog of the Treaties and as stakeholder in the global debate about internet governance, should demand in the upcoming international fora, and beyond September 2015 as ICANN potential member, that ICANN fully respect the rights of European citizens and domain names owners.

We therefore expect that the European Commission, and more specifically you, as the Commissioner for Digital Agenda, will address ICANN's violation of EU Data Protection laws policy and place the issue on the negotiations agenda. Concrete actions can easily be taken, and the next fora, namely the Ninth Annual Internet Governance Forum (IGF) Meeting to be held in Istanbul, Turkey on 2-5 September 2014, provides a great opportunity for the EU to prove its attachment to the protection of private life of all citizens.

A full memorandum, with annexes, is attached for your consideration. We of course remain at your disposal should you or your staff have any questions.

Yours faithfully,

For eLabEurope
Alberto Alemanno
www.eLabEurope.eu
@elabeurope

*ICANN and the Internet Governance Reform*

The issue of ICANN's violation of the Data Protection Directive provides further impetus to the ongoing efforts relating to Internet Governance Reform, which has regularly been advocated over the past few years. Freedom, non-discrimination and respect for human rights emerge today as the core values of the web. Its diverse stakeholders and major actors have consistently demanded a "COMPACT[1] Internet" based on a few basic principles including responsibility of users, multi-lateral governance, confidence, transparency and democracy.

The problem of the international governance is today epitomized by the ICANN privacy issue. It proves that the Internet cannot be regulated through a national organization, and that all legal links with a state entity must therefore be broken. In these circumstances, one of the main challenges is the use made of Big Data.

The implication of the European Union is essential both domestically, with the need to reach a Digital Single Market and abroad, in order to tackle issues such as cyber-criminality while at the same time ensuring the protection of citizens' fundamental rights. The promotion of an internationally regulated Web must be maintained, particularly through the Internet Governance Forum established by the United-Nations Secretary-General in July 2006 to discuss security, diversity, and access to the Internet. **In the aftermath of the NETMundial Conference, the next IGF in Turkey (September 2014), in particular, provides a great opportunity for the EU, and particularly the Commission, to express its views and opinions on the Internet Governance and the necessary reform of ICANN.**

*Why ICANN's Data Retention specification needs to be amended*

In June 2013, ICANN issued an updated 2013 Registrar Accreditation Agreement (RAA). Under the subsection titled "Data Retention Specification," registrars are required to collect information from registrants and maintain that information for two years after the registrant terminates the relationship with the registrar, i.e. stops paying the fees for using a domain name. If the registrar believes that fulfilling the requirement would violate any laws, then the registrar has the option of filing a waiver by submitting a "written legal opinion."

Before the 2013 RAA came into effect, the Article 29 Data Protection Working Party of the European Commission (hereinafter "Working Party") published a statement directed towards ICANN regarding the legality of the Data Retention Specification. The Working Party wished to "provide a harmonized statement concerning compliance with European data protection law" reflecting the unified opinion of the 27 (now 28) national data protection authorities.

On September 20, 2013, the General Counsel of ICANN responded to the Working Party by stating that the Data Retention Specification serves the purpose of "helping registrants resolve problems related to their domain name accounts with Registrars." The General Counsel also stressed that the RAA does not create any new mechanisms by which law enforcement personnel can access

[1] COMPACT : "Civic responsibility- One Internet- Multi-stakeholder governance- Pro-democracy- Architecture matters- Confidence of users- Transparent governance"-Neelie Kroes, 28/06/2011

billing information, and that law enforcement is still required to follow applicable law if it wishes to access the information.

On January 8, 2014, the Working Party issued another statement that the RAA violates Article 6(e) of the European Data Protection Directive 95/46/EC which states that personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected. Although addressed in ICANN's September 20, 2013 letter, the 2013 RAA does not specify a legitimate purpose for keeping the data for an additional two years.

On April, 17, 2014, less than ten days after the Court of Justice of the European Union declared for similar reasons the Data Retention Directive to be invalid[2], the European Data Protection Supervisor sent a letter to ICANN's General Counsel complaining that their answers does not "address sufficiently our concerns which were raised between the Working Party and ICANN on the retention periods and data collection".[3]

**We, at eLabEurope, would like to support this view, and request that the full compliance with EU law for be incorporated in the EU Commission position towards ICANN's reform.**

*How ICANN violates the Data Protection Directive*

The information required to be retained under the ICANN Data Retention Specification, detailed by the *Description of the 2013 RAA Data Retention Specification Data Elements and Legitimate Purposes for Collection/Retention Discussion Draft*[4] released on Mar, 21st 2014, which includes the registrant's full name, contact information, and credit card and billing information, and types of services used, linked to the domain name he/she was owning, is unequivocally personal data as defined in Article 2 of, and therefore protected under, the Data Protection Directive (Directive 95/46/EC). The European Court of Justice has previously ruled that an individual's contact information,[5] and even simply a person's name[6], amounts to personal data for the basic reason that it allows an individual to be identified. Moreover, we believe that credit card and billing information, although not explicitly defined as a "special category of processing" under the Directive[7], should be considered highly sensitive information because, particularly in light of real risks of identity theft due to malicious system breaches, such information can potentially reveal or allow access to an individual's financial assets. Sensitive information could also be involved in case the domain name referred to registrants' political views, religion, sexual orientation, etc.

---

[2] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014]

[3] Available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2014/14-04-17_EDPS_letter_to_ICANN_EN.pdf

[4] http://www.icann.org/en/resources/registrars/raa/draft-data-retention-spec-elements-21mar14-en.pdf

[5] *See* Case C-101/01 *Criminal Proceedings against Bodil Lindqvist* [2003]

[6] *See* Case C-28/08 P *European Commission v The Bavarian Lager Co. Ltd* [2010] ECR I-6055.

[7] *See* Article 8, Directive 95/46/EC.

It should be noted that the fact that web domains often serve a business function does not make registrars any less deserving of protection under current EU law. If we look at the judges from Strasbourg, the European Court of Human Rights held that the retention of data relating to professional communications falls within the scope of "private life" under the relevant provision of the Europe Convention of Human Rights.[8] In this way, the European Court of Human Rights found there was no distinction between activities of professional and those of private nature for purposes of personal data protection.[9] The European Court of Justice has now also embraced this broad interpretation of "private life," holding that professional and business activities are not excluded from the concept of private life.[10] Registrants of web domains, whether they use such services for personal or business purposes, are guaranteed equal data privacy rights under the Directive.

Under the Data Protection Directive, data may be stored[11] only if one of the enumerated conditions is met.[12] ICANN cannot demonstrate that it meets any of these conditions. ICANN does not meet the consent condition, since registrants are not given the option to consent or object to the retention of their personal data under the Data Retention Specification.[13] Indeed, registrants are not privy to the Registrar Accreditation Agreement, but are subject to data retention due to their registrar's agreement with ICANN alone. Nor can ICANN meet the condition under which the data processing is necessary for the performance of a contract.

Individual registrants are not privy to the relevant contract, and moreover the data retention at issue continues for two years after the registrant's contractual relationship terminates (i.e. the registrant abandons the web domain).[14] Certainly, ICANN can neither claim to require such data retention for purposes of fulfilling its own legal obligations.[15] Nor can the policy have a purpose of protecting "vital" interests of the data subject.

ICANN has argued that, despite the lack of any legal obligation or consent by data subjects from which to base this mandatory data retention, its policy is nevertheless based on the legitimate purpose of ensuring that former web domain name holders can resolve billing and other issues with their former registrars. To make this argument, ICANN must prove that the benefits of its data retention policy outweigh the resulting privacy interferences caused,[16] and that the personal data is stored for no longer than is absolutely necessary for the asserted purposes.[17] The Article 29 Working

---

[8] ECHR, Amann v. Switzerland [GC], No. 27798/95, 16 February 2000, para. 65.
[9] *Id.*
[10] General Court decision, T-194/04, 8.11.2007.
[11] Article 2 of Directive 95/46/EC expressly includes collecting and storing data within the definition of data processing.
[12] *See* Article 7, Directive 95/46/EC.
[13] *See* Data Retention Specification, *available at* http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm#data-retention.
[14] *Id.*
[15] Registrars are not required by the 2006/24/EC Directive (the "Data Retention Directive") because that Directive imposes obligations only on electronic communication providers which do not include web domain registrars.
[16] Article 7(f) of the Data Protection Directive allows the processing of personal data for legitimate purposes on the condition that such purposes are not outweighed by data subjects' fundamental rights.
[17] Article 6(1)(e) of the Data Protection Directive requires that personal data is retained, assuming it is done so according to a legal basis, for no longer than is absolutely necessary for the purposes asserted.

Party has repeatedly declared that the benefits asserted by ICANN are disproportionate to the risks for individuals and their rights to be assured their personal data is protected.[18]

**eLabEurope is of the opinion, in line with the Article 29 Working Party, that the ICANN's two-year retention period is patently excessive and unnecessary and therefore violates Article 6 and 7 of the EU Data Protection Directive**.

**We believe this to be especially so in light of the growing global risk of malicious system breaches** that increasingly results in massive thefts of individuals' personal data. For example, in December of 2013 the major U.S. retail store, Target, was the victim of a major system breach that resulted in the theft of credit card and personal information belonging to an estimated 70 million to 110 million individuals.[19] Heartbleed security bug is also a good recent example. Web domain registrars undoubtedly face the same risks. As reported widely in January of 2014, GoDaddy.com, an American registrar under ICANN's governance policies, was victim of a breach resulting in an intruder gaining access to and compromising a registrant's valuable social media accounts and profiles.[20]

There are currently 135 registrars based in EU Member States that are subject to ICANN's RAA agreement.[21] These registrars are very diverse in size, and more importantly are diverse in their security apparatuses. A standard period of time mandated for all 135 registrars regardless of their technical security measures and capacity is arbitrary and cannot be deemed necessary in every instance. Whereas in the case of large registrar with highly secure data systems, a two year data retention period may not result in a disproportionate risk to an individual's data privacy. However, in the case of a small registrar that lacks highly secure systems, the risk to data privacy and security caused by a two-year period will outweigh ICANN's asserted purpose of assuring convenience in resolving billing disputes following contract termination.

In short, the two-year data retention time period following contract termination is neither proportionate nor necessary when applied all 135 web domain registrars in light of the potential for misuse of personal data. As the Article 29 Working Party has repeatedly asserted, due to the excessive data retention period required by its Data Retention Specification, ICANN is in violation of Article 6's requirement that data is retained for no longer than is absolutely necessary. Moreover, due to the disproportionate risks to privacy and security over individuals' personal data, ICANN is in violation of Article 7's requirement that the asserted purpose of data retention is not outweighed by data subjects' privacy rights.

---

[18] *Letter from Article 29 Working Party to ICANN,* 06 June 2013, *available at* http://www.icann.org/en/news/correspondence/kohnstamm-to-crocker-chehade-06jun13-en.pdf

[19] *For Target, the Breach Numbers Grow*, New York Times, Jan. 10, 2014, http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?action=click&module=Search&region=searchResults%230&version=&url=http%3A%2F%2Fquery.nytimes.com%2Fsearch%2Fsitesearch%2F%3Faction%3Dclick%26region%3DMasthead%26pgtype%3DHomepage%26module%3DSearchSubmit%26contentCollection%3DHomepage%26t%3Dqry485%23%2Ftarget%2Bbreach%2F&_r=0.

[20] The story cited is notable because the registrant's social media account was valued at roughly fifty thousand dollars prior to being stolen. *Man claims hacker took Paypal, GoDaddy accounts hostage in exchange for his $50G Twitter handle*, @N, New York Daily News, Jan. 29, 2014, http://www.nydailynews.com/news/national/man-online-accounts-held-hostage-twitter-handle-victim-article-1.1596119.

[21] ICANN-Accredited Registrars, last accessed March 30 2014, http://www.icann.org/registrar-reports/accredited-list.html.

As the European Data Protection Supervisor rightly pointed out in his correspondence to ICANN, "it is reasonable to expect requirements for retaining personal data to be subject to increasing scrutiny and legal challenges in the EU", all the more so since member of the European Parliament are currently discussing a General Data Protection Regulation, which would be stricter and directly applicable.

*ICANN's Data Retention policies must be addressed by the EU*

Under the ICANN's current RAA, an individual registrar may request a waiver from complying with the Data Retention Specification in the event it is believed that it would violate applicable governing law.[22] eLabEurope is of the opinion that allowing ICANN to maintain its individual waiver procedure within the European Union is counter to the principle of enforcing data protection laws throughout the continent.[23]

Indeed, OVH SAS, a large French registrar, recently requested and was granted a partial waiver from the Data Retention Specification on the ground that the two year retention period violated both French and European Law.[24] In its waiver request, OVH SAS pointed to the EU Data Protection Directive, as well as to two French laws. The first French law is an exact transposition of the Data Protection Directive,[25] and the second French law cited stipulates that the personal data at issue must be retained for one year following contract termination.[26] It is presumably the latter law that OVH SAS based its request for a partial waiver constituting a one-year retention period. As a result, ICANN agreed to allow OVH SAS and all French web domain registrars to limit their personal data retention to one year.

It is contradictory to a harmonized system of data privacy that web domain registrars in one Member State are required to retain personal data for two years following contract termination, and registrars in another Member State are restricted to retaining personal data to one year, for the exact same service. An individualized waiver system subject to the sole discretion of ICANN creates a situation in which existing EU data protection laws may be enforced heterogeneously across the EU. If ICANN is allowed to maintain its waiver scheme as a mechanism for ensuring compliance with European law, then the waiver should apply uniformly to all registrars operating within the European Union. In the alternative, ICANN should be instructed to abandon its two-year data retention policy in its Registrar Accreditation Agreement. In any case, as the Working Party states, **regulations on data retention should not be generally defined by a contract issued by a private company, but by the legislator acting on behalf of the citizens' interest.**

---

[22] *See* Data Retention Specification, *available at* http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm#data-retention.

[23] Furthermore, paragraph 65 of the Preamble of Directive 95/46/EC identifies a primary objective of the Article 29 Working Party as the unification of the applicable of national data protection laws.

[24] *OVH SAS Data Retention Specification Waiver Request*, *available at* http://www.icann.org/en/resources/registrars/updates/retention/waiver-request-ovh-sas-27jan14-en.pdf.

[25] Article 6, La Loi 78-17 du 6 Janvier 1978, *available at* http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/.

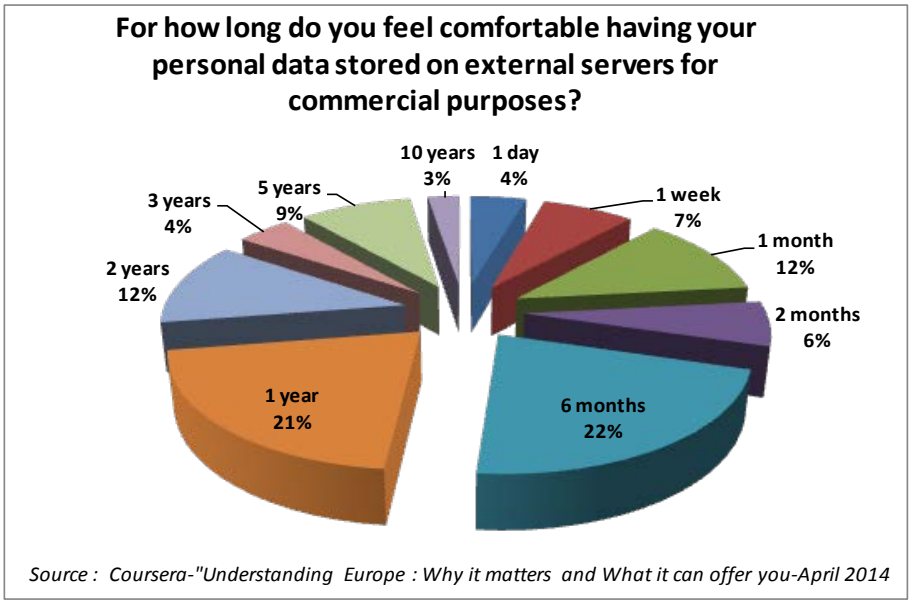
[26] Article 3, Décret n° 2011-219 du 25 février 2011

*Conclusions*

The European Union could gain legitimacy towards its citizens if its institutions and representatives commit to addressing public interest matters and tackle them efficiently. eLabEurope strongly wishes to be part of this endeavor. As a nonpartisan organization committed to promoting civic engagement through academic research and consultancy to the public interest, we are dedicated to protecting individual rights within the European Union and thus contribute to the building of a new democratic space.

We strongly believe that civil society should be granted a strong role in building the new model of Internet Governance currently being discussed today at the international level. In such matters, citizens should be entitled to directly have their say.

Thanks to our 40,000 MOOC participants on Coursera, we were able to carry out a survey reflecting the concerns of citizens regarding the protection of their own personal data.




*Source : Coursera-"Understanding Europe : Why it matters and What it can offer you-April 2014*

As seen on the pie chart above, only 12% of survey respondents felt comfortable with their personal data being stored for two years, as required under ICANN's data retention policy. Even a smaller percentage of survey respondents felt comfortable with the storage of personal data for a longer period of time.

**44% of respondents would feel comfortable with their personal data being stored 6 months or one year, which is exactly what OVH has been granted** (6 months for sensitive data like phone numbers that may have been collected during the subscription, and one year – reduced from two – for name and credit card number). In fact, a majority (51%) of respondents would prefer their data to be stored 6 months or less.

**Thus, asking ICANN to automatically and immediately grant all EU operators the same condition as OVH would already be a step in the right direction.**

As the Commission has argued several times, a global reform of Internet governance will then be necessary to increase individual protections of personal data. The Commission has taken a first position on ICANN's reform and Internet governance, adding further that the Parliament and the Council will also discuss the issue.

**We believe that the negotiation around Internet governance should also encompass the protection of registrant's personal data, and that this particular point should clearly appear in the positions taken by the EU institutions on ICANN's reform.**

Therefore, we would like to kindly ask you to include a discussion of ICANN's compliance with (current and future) EU data protection law into the more general agenda the EU Commission will be defending regarding internet governance over the next months. The global negotiation around ICANN's evolution is a one-time opportunity to make the fundamental rights of European citizens online respected. The EU must seize it.

**Annex 1: ICANN Grants Data Retention Waiver to OVH SAS**

12 March 2014

DATA RETENTION WAIVER
OVH SAS

OVH SAS ("Registrar") submitted to ICANN a Registrar Data Retention Waiver Request ("Waiver Request") on the basis of Registrar's contention that compliance with the data collection and/or retention requirements of the Data Retention Specification in the 2013 RAA violates applicable law in France.

ICANN hereby grants Registrar a limited waiver from compliance with certain provisions of the 2013 RAA on the following terms:

1. ICANN agrees that, following Registrar's execution of the 2013 RAA, for purposes of assessing Registrar's compliance with the data retention requirement of Paragraph 1.1 of the Data Retention Specification in the 2013 RAA, the period of "two additional years" in Paragraph 1.1 of the Data Retention Specification will be deemed modified to "one additional year."
2. In all other respects the terms of the Data Retention Specification will remain AS-IS. The waiver granted to Registrar applies only to the post-sponsorship period of retention of the data listed in the Paragraphs 1.1.1 through 1.1.8 inclusive of the Data Retention Specification, and it does not constitute a waiver of any other provisions of the 2013 RAA or other ICANN policies applicable to registrars. Without limiting the foregoing, nothing in this waiver limits Registrar's obligation to comply with Consensus Policies or Temporary Policies developed and adopted in accordance with ICANN's Bylaws ("ICANN Policies") or limits Registrar's obligation to comply with any amendment, supplement or modification of the 2013 RAA approved and adopted in accordance with the terms of the 2013 RAA("RAA Amendments"). In the event of any inconsistency between this waiver and the terms of any ICANN Policy or RAA Amendment, the terms of the ICANN Policy or RAA Amendment will control.
3. The waiver granted to Registrar shall remain in effect for the duration of the term of the 2013 RAA signed by Registrar.

# Annex 2: Letter from Article 29 Working Party to ICANN, 06 June 2013



**ARTICLE 29 Data Protection Working Party**

Brussels, 06 June 2013

Dr. Steve Crocker and Mr. Fadi Chehadé
Chairman and 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: Statement on the data protection impact of the revision of the ICANN RAA**

Dear Mr Crocker and Mr Chehadé,

In the context of ICANN' s revision of the Registrar Accreditation Agreement (RAA) and the final **RAA Proposal**[1], the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Article 29 WP)[2] wishes to provide a harmonised statement concerning compliance with European data protection law.

Following up on our letter of 27 September 2012[3] and previous contributions to the process of collecting and disclosing WHOIS data[4], this statement specifically addresses the legitimacy of the data retention obligation for registrars, contained in the new RAA.

The Working Party notes that ICANN has included a procedure for registrars to request a waiver from these requirements if necessary to avoid a violation of applicable data protection law. Such a waiver request can be based on written guidance from a governmental body of

[1] ICANN Proposed Final 2013 RAA of 22 April 2013, URL: http://www.icann.org/en/news/public-comment/proposed-raa-22apr13-en.htm

[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. It is composed of representatives from the national data protection authorities of the EU Member States, the European Data Protection Supervisor and the European Commission. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/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] Article 29 Working Party letter to ICANN, 26 September 2012, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120926_letter_to_icann_en.pdf

[4] URLs: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp76_en.pdf , http://www.icann.org/correspondence/schaar-to-cerf-22jun06.pdf and http://gnso.icann.org/correspondence/schaar-to-cerf-12mar07.pdf

competent jurisdiction providing that compliance with the data retention requirements violates applicable law.

In order to avoid unnecessary duplication of work by 27 national data protection authorities in Europe, with this letter, the Working Party wishes to provide a single statement for all relevant registrars targeting individual domain name holders in Europe.

The final proposed Data Retention specification roughly distinguishes between name and contact details for the domain name holder (specified in 1.1.1 to 1.1.7) and all other types of data a registrar might collect (specified in 1.2.1 to 1.2.3), such as logfiles and billing records containing the 'means and source of payment', logfiles about the communication with the registrar including source IP address, telephone number, e-mail address, Skype handle or instant messaging identifier, as well as the date, time and time zones of communications.

Registrars are required to keep the first category of personal data for a period of two years after the contract for the domain has been ended. The second category of personal data must be retained for six months after the contract has ended.

The first category of data includes payment data, defined as: *'card on file', current period third party transaction number, or other recurring payment data.*

The proposed new data retention requirement does not stem from any legal requirement in Europe.[5] It entails the extended processing of personal data such as credit card and communication data by a very large number of registrars. The fact that these data may be useful for law enforcement (including copyright enforcement by private parties) does not equal a necessity to retain these data after termination of the contract. Taking into account the diversity of these registrars in terms of size and technical and organisational security measures, and the chance of data breaches causing adverse effects to individuals holding a domain name, the Working Party finds the benefits of this proposal disproportionate to the risk for individuals and their rights to the protection of their personal data.

Secondly, the Working Party reiterates its strong objection 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 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.[6]

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. Because there is no legal ground for the data processing, the proposed data retention requirement violates data protection law in Europe.

---

[5] 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.

[6] 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).

In general, we repeat that 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. In that light, the Working Party welcomes the growing number of registries in Europe that are offering layered access to the WHOIS data.

Yours sincerely,

On behalf of the Article 29 Working Party,

Jacob Kohnstamm
Chairman