

ARTICLE 19

# ICANN's Corporate Responsibility to Respect Human Rights

---

February 2015

ARTICLE 19  
Free Word Centre  
60 Farringdon Road  
London  
EC1R 3GA  
United Kingdom  
T: +44 20 7324 2500  
F: +44 20 7490 0566  
E: [info@article19.org](mailto:info@article19.org)  
W: [www.article19.org](http://www.article19.org)  
Tw: [@article19org](https://twitter.com/article19org)  
Fb: [facebook.com/article19org](https://facebook.com/article19org)

© ARTICLE 19, 2015

This report is a publication of ARTICLE 19: Global Campaign for Free Expression. It was written by Dr. Monika Zalnieriute, from the Centre for Internet & Human Rights, European University, Viadrina, Berlin, with input from Gabrielle Guillemin, Senior Legal Officer of ARTICLE 19, Niels ten Oever, Head of Digital of ARTICLE 19 and Emily Hislop, Intern of ARTICLE 19's Law Programme.

This work is provided under the Creative Commons Attribution-Non-Commercial-ShareAlike 2.5 licence. You are free to copy, distribute and display this work and to make derivative works provided you:

1. give credit to ARTICLE 19
2. do not use this work for commercial purposes
3. distribute any works derived from this publication under a licence identical to this one.

To access the full legal text of this licence, please visit: <http://creativecommons.org/licenses/by-nc-sa/2.5/legalcode>.

ARTICLE 19 would appreciate receiving a copy of any materials in which information from this document is used.

# Table of Contents

---

Executive summary ..... 4

Recommendations ..... 4

Introduction ..... 5

UN Guiding Principles on Business and Human Rights & Due Diligence ..... 6

New gTLDs and Freedom of Expression..... 7

The *Applicant Guidebook* on new gTLDs raises issues for freedom of expression ..... 7

ICANN’s corporate responsibility to respect freedom of expression..... 8

The RAA, Privacy and Data Protection ..... 10

The RAA data retention clause and public access policy are inconsistent with international data protection principles..... 10

The data retention clause ..... 10

The WHOIS database and public access policy..... 10

ICANN must respect the right to privacy and data protection principles ..... 10

Conclusion..... 12

Endnotes ..... 13

# Executive summary

---

Freedom of expression and privacy are internationally recognised human rights. This paper addresses the privacy and freedom of expression issues that arise in relation to the Internet Corporation for Assigned Names and Numbers (ICANN) policies and procedures. In particular, it explores the corporate responsibility of ICANN to respect human rights. In this sense, it seeks to develop and go beyond the Council of Europe report published in June 2014, which explored the duty of governments – rather than corporations - to protect human rights.<sup>i</sup>

Moreover, unlike the purely European perspective adopted in the Council of Europe report, this paper addresses the human rights issues that arise from a global perspective in relation to ICANN's policies and mechanisms. Taking into account ICANN's global reach, it refers only to the international human rights documents that do not pertain to any particular continent or legal tradition. In particular, it relies on the *UN Guiding Principles on Business and Human Rights* (Guiding Principles), known as the 'Protect, Respect, and Remedy' framework,<sup>ii</sup> which were unanimously adopted by the United Nations Human Rights Council in June 2011.

This paper sets out the UN Guiding Principles and explains their relevance to ICANN's policies and procedures on new generic Top Level Domains (gTLDs) and the *Registrar Accreditation Agreement* (RAA). In particular, it examines the ways in which ICANN's standards and policies governing the 'sensitive applied-for strings' fall short of freedom of expression standards, and, furthermore, how the RAA provisions are in breach of data protection best practices and standards.

## Recommendations

In line with the UN Guiding Principles and the human rights due diligence process, ICANN should:

1. weigh the human rights impact of its policies and procedures;
2. develop strategies to ensure that staff and other stakeholders understand this impact;
3. develop and articulate a human rights policy, and make sure employees and other stakeholders know, understand and implement it;
4. develop metrics to monitor ICANN's human rights performance.

# Introduction

---

The Internet Corporation for Assigned Names and Numbers (ICANN) is a unique multi-stakeholder body, responsible for the technical management of Internet domain names and addresses. It operates at a global level and creates policy governing the introduction of new generic Top Level Domains (gTLDs) into the DNS. Domain names often entail expressive and communicative elements (e.g. .gay, .sucks, .islam and so on),<sup>iii</sup> so ICANN's policies are directly relevant to the right to freedom of expression.<sup>iv</sup> Furthermore, the relationship between ICANN and the domain name registrars is governed by the 2013 *Registrar Accreditation Agreement* (RAA), whose data retention and disclosure provisions are relevant to the right to data privacy and data protection. In short, ICANN's policies and procedures may substantially interfere with the enjoyment of a range of internationally recognised human rights under the *Universal Declaration of Human Rights* (UDHR), the *International Covenant on Civil and Political Rights* (ICCPR) and the *International Covenant on Economic, Social and Cultural Rights* (ICESCR).<sup>v</sup>

At the same time, ICANN is a non-profit corporation registered in California and therefore subject to US law. As a private company, it is not bound by the US *Bill of Rights*. Nor can it be held liable under international human rights law, which is directly binding only upon states. Nonetheless, as a corporation whose policies have a strong impact on matters of public interest and infrastructure well beyond US borders, ICANN has a responsibility to respect human rights, according to the *UN Guiding Principles on Business and Human Rights* (the Guiding Principles).<sup>vi</sup>

Thus, not only does ICANN have the potential to interfere with human rights, it also has a responsibility under international law not to do so. Moreover, under Article 4 of the Articles of Incorporation, ICANN is bound to operate “*for the benefit of the Internet community as a whole, carrying out its activities in conformity with relevant principles of international law and applicable international conventions and local law*”.<sup>vii</sup>

With this in mind, this paper analyses the ways in which the Guiding Principles can contribute to the development of policies and processes within ICANN to protect the rights to freedom of expression and privacy. It is hoped that it will further the cross-community debates on ICANN & human rights within ICANN policy circles, which will result in some tangible policy changes and reforms.

This paper is divided into three parts. Part I sets out and explains the *UN Guiding Principles on Business and Human Rights*. Part II examines the freedom of expression issues that arise in relation to the new gTLDs and how the Guiding Principles should apply in that context. Part III explains the implications of the RAA for the right to privacy and the way in which the Guiding Principles can assist in that context.

# UN Guiding Principles on Business and Human Rights & Due Diligence

---

The *UN Guiding Principles on Business and Human Rights* were endorsed by the United Nations Human Rights Council in June 2011. They apply to corporations, partnerships, and any other legal forms used to establish business entities, regardless of size, sector, location, ownership and structure. As noted above, ICANN's status as a non-profit corporation clearly falls under the broad notion of 'other business enterprises' under the Guiding Principles.<sup>viii</sup>

The UN Guiding Principles 'are grounded in recognition of the role of business enterprises as specialized organs of society performing specialized functions, required to comply with all applicable laws and to respect human rights.'<sup>ix</sup> Thus, ICANN has a duty to respect human rights obligations: 'this means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.'<sup>x</sup> This corporate responsibility is applicable regardless of frontiers, throughout global operations, irrespective of where registrars, users, and domain name owners are located. The *Organisation for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises* further explain that "[a] State's failure either to enforce relevant domestic laws, or to implement international human rights obligations or the fact that it may act contrary to such laws or international obligations does not diminish the expectation that enterprises respect human rights. In countries where domestic laws and regulations conflict with internationally recognized human rights, enterprises should seek ways to honour them to the fullest extent which does not place them in violation of domestic law".<sup>xi</sup>

Under the UN Guiding Principles, companies operating in the ICT sector are expected to adopt an explicit policy statement outlining their commitment to respect human rights both substantially and procedurally throughout their activities; and also to put in place appropriate due diligence mechanisms which identify, assess, and prevent any adverse impact on human rights. In the context of ICANN, the Guiding Principles support the creation of a body dedicated to human rights protection – e.g. a human rights advisory council - which would assess whether ICANN's policies, procedures and complaints mechanisms are compatible with international human rights standards, in particular those concerning the right to freedom of expression and the right to data privacy. In case of non-compliance, the body in question would make recommendations as to how such shortfalls might be remedied. Currently, there is no such body within ICANN, and this paper aims to contribute to the on-going discussion and highlight several existing ICANN policies and mechanisms that may adversely affect internationally recognised human rights. In particular, the paper examines the ways in which ICANN's standards and policies governing the 'sensitive applied-for strings' may fall short of international freedom expression requirements, and shows how the RAA provisions may come at the expense of data privacy considerations.

# New gTLDs and Freedom of Expression

---

One of the core functions of ICANN is to lay down policy governing the introduction of new gTLDs into the DNS. As noted above, domain names often entail expressive and communicative elements.<sup>xii</sup> In particular, ICANN's decisions as to whether or not to approve applications for new gTLDs such as .porn, .fail or .islam, can have an impact on the accessibility of information on the Internet. Such judgements are not dissimilar to the editorial judgements made by publishers who routinely decide what content to publish in line with editorial policies or business interests and who, in certain cases, have to consider what content is relevant for the purpose of serving the public's right to know. In other words, ICANN makes some content-related judgements, which could have an impact on Internet content availability. Domain name policy therefore has clear implications for the right to freedom of expression, as recognised by the Governmental Advisory Committee (GAC) in its San Francisco Communiqué.<sup>xiii</sup> In practice, most freedom of expression issues arise in the course of various procedures that can be followed in order to object to an application for a new gTLD.

## **The *Applicant Guidebook* on new gTLDs raises issues for freedom of expression**

The *Applicant Guidebook* (Guidebook) provides for five types of procedures that may be relevant to an application for a new gTLD where there are various sensitivities or public objections involved. Each of these procedures may have implications for freedom of expression.

- **Ineligible or prohibited words:** the Guidebook contains a list of words which are 'ineligible for delegation'.<sup>xiv</sup> This constitutes a content-related choice, made a priori by ICANN, which is expected to result in content-related judgements whenever questions involving usage of any of those ineligible words may arise. The use of the words 'olympic', 'redcross' and their variations are also prohibited. This blanket prohibition constitutes a restriction on the right to freedom of expression, and would likely fail the proportionality test applied under international human rights law.
- **The string review procedure:** this procedure is designed to determine whether an applied-for gTLD string might have an adverse impact on DNS stability and security, which might consequently lead to non-approval of the new gTLD.<sup>xv</sup> An evaluation of adverse impact is likely to include a 'TLD-blocking or filtering impact assessment' due to 'sensitive expression' included in the applied-for strings. This was the case in deliberations on the controversial '.xxx' TLD, where the ICANN Board stated that the risk of blocking did not justify non-approval of that string.<sup>xvi</sup> In practice, such impact assessments cannot be separated from considerations as to what is regarded as 'useful or harmful' by different communities and Internet users around the world. This is again highly relevant to the protection of the right to freedom of expression.
- **GAC 'Early Warning' and 'Advice' procedures:** the GAC can express its views on specific new TLDs on the grounds that the TLD is potentially sensitive or problematic for one or more governments, via two distinct procedures: (1) 'Early Warning' and (2) 'Advice' to the ICANN Board. The Early Warning is a notice from members of the GAC that an application is deemed potentially sensitive or problematic by one or more states. An Early Warning is "not a formal objection, nor does it directly lead to a process that can result in rejection of the application."<sup>xvii</sup> For instance, ICANN has received over 240 comments from various governments around the world, issued as Early Warnings from the GAC, such as for the strings .fail, .gripe, .sucks, and .wtf due to their "overtly negative or critical connotation".

The GAC can also give 'Advice' to the ICANN Board regarding an application identified as problematic, such as one that potentially violates national law or raises sensitivities. National and religious concerns have been raised by various governments on several occasions. For example, the UAE government expressed serious concern with regard to .islam on grounds of lack of community involvement and support as well as private control over the name. Concerns were also raised over strings relating to a regulated market sector, such as .accountant, .lawyer

and .doctor, where misuse can potentially result in serious harm to consumers. These examples demonstrate the complex and sensitive nature of such procedures, which raise a number of human rights issues relating to the exercise of freedom of expression, freedom of association and freedom of religion.

- **The dispute resolution procedure:** this procedure can be triggered by a formal objection to an application by a third party (usually a trademark owner).<sup>xxiii</sup> The public objection procedures include: (1) the string confusion objection; (2) the legal rights objection; (3) community objection; and (4) limited public interest objection.<sup>xxix</sup>

A gTLD objected to under a string confusion objection must qualify as confusingly similar to an existing gTLD or a gTLD which was applied for in the same application round.<sup>xx</sup> A legal rights objection can occur when an applied-for gTLD infringes on the intellectual property rights of the objector, who must have a legal right over the disputed domain name in order to have standing for this objection.<sup>xxi</sup> These two objections grounds for initiating dispute resolution procedures are focused on the protection of traditional trademark rights, whereas the third and fourth objections concern communities. Actual examples usually include offensive expression - political, commercial and non-commercial – made possible by gTLDs such as .sucks or .fail to follow, for example, a surname of a well-known politician or brand. The community objection ground for refusal was used in relation to the case of .xxx, which relates to cases in which “there is a substantial opposition to the gTLD application from a significant portion of the community to which the gTLD string may be explicitly or implicitly targeted.”<sup>xxii</sup> This case illustrates the complex balance between freedom of expression and the property rights of trademark owners, as well as community interests.

- **The ‘string contention procedure’:** this procedure can be used in circumstances where applied-for gTLDs are either identical or similar enough to cause consumer confusion.<sup>xxiii</sup> A string contention occurs either when (1) two or more applicants for an identical gTLD successfully complete previous evaluation and dispute resolution stages - most notably the objections period - or (2) when two or more applicants for a similar gTLD complete all previous stages and ICANN considers the gTLDs create the probability of causing (consumer) confusion.<sup>xxiv</sup> Under the string contention procedure, communities are given precedence in the case of the TLDs in contention. Precedence is automatically taken if the community applicant passes the so-called ‘community priority evaluation’ (CPE). Let us take as an example a case in which there are four applicants for the .gay gTLD, of which three are standard applicants and one is a community applicant, but the CPE process is still ongoing and it is unclear whether a community applicant - dotgay LLC – will be given priority. In most cases where multiple applicants apply for a single new gTLD, it is expected that contention will be resolved using the community priority evaluation, or through a voluntary agreement between the involved applicants. If that is not the case, auctions will take place to determine the winner of each contention set.<sup>xxv</sup> The CPE process and the auctions, similar to other string evaluation procedures, may have a direct impact on Internet content availability, and they clearly overlap with issues relating to the exercise of the right to freedom of expression, the freedoms of association and religion, as well as the principle of equality and non-discrimination.<sup>xxvi</sup>

## ICANN’s corporate responsibility to respect freedom of expression

Compliance with the UN Guiding Principles would assist ICANN in addressing the issues outlined above. To begin with, and in line with the Guiding Principles, ICANN should develop policies outlining its commitment to the prevention, assessment, and mitigation of threats to freedom of expression associated with the new gTLDs. This would include a commitment by ICANN to conduct regular human rights impact assessments in order to fulfil its due diligence obligations. A human rights body (AHRC) would ensure that ICANN abides by those commitments.

Human rights policies and oversight would be especially useful in the context of government objections to certain gTLDs. As the objections to e.g. .gcc, .africa, .islam demonstrate, GAC and governments play an important role concerning new gTLDs within ICANN procedures. By putting mechanisms in place to



evaluate and handle government requests that may have an impact on freedom of expression, ICANN would ensure that such requests are independently reviewed in accordance with internationally recognised human rights standards. This could include the ability for the human rights reviewer to consult the relevant authorities (such as, e.g, information commissioners, etc.) in order to seek clarification or modification in appropriate cases.

Guaranteeing the right to freedom of expression is an integral part of ICANN's duty to act in the global public interest under Article 4 of the Articles of Incorporation. At a minimum, the due diligence principle, as defined by the UN Guiding Principles, requires that ICANN should engage in meaningful consultation with relevant stakeholders as to the means by which ICANN can fulfil its human rights obligations. Such consultation should not only take place within the ICANN community but should extend more broadly to affected stakeholders, such as the media, NGOs, the UN or other relevant supranational bodies. In the context of new gTLDs, such consultations should lead to the establishment of appropriate mechanisms which can ensure the protection of freedom of expression.

# The RAA, Privacy and Data Protection

---

ICANN's policies have the capacity to interfere not only with freedom of expression, but also with the right to privacy and data protection. This is especially true of the 2013 RAA, which governs the relationship between ICANN and domain name registrars. In particular, the RAA 2013 contains 'data retention' and 'public access to data on registered names' clauses, which are highly problematic from the perspective of data protection and the right to privacy.

## **The RAA data retention clause and public access policy are inconsistent with international data protection principles**

### **The data retention clause**

Under the 2013 RAA, registrars are required to make available a variety of personal data about domain names (referred to formally as Registered Names) and their owners (Registered Name Holders), which are retained by private companies for up to two years after the contract for the domain has ended.

This data retention clause seems to be incompatible with numerous requirements outlined in international data protection instruments, including the *UN Guidelines*,<sup>xxvii</sup> the *OECD Guidelines*,<sup>xxviii</sup> and the *Madrid Resolution*,<sup>xxix</sup> as well as regional data protection frameworks, such as the *Council of Europe Convention 108*,<sup>xxx</sup> the *Asia-Pacific Economic Cooperation (APEC) Privacy Framework*,<sup>xxxi</sup> and the *EU Data Protection Directive*.<sup>xxxii</sup> In particular, the 2013 RAA fails to specify the legitimate purpose for which the data was collected. Furthermore, there is no legal duty, under international law or otherwise, binding ICANN to store personal data after the termination of the contract for law enforcement purposes.

Given that ICANN is able to amend RAA rules at any time, it is unclear why the data retention provisions have not been amended so that personal data is retained for no longer than is necessary for the performance of the contract. Moreover, if governments wish to collect personal data for law enforcement purposes, they are free to establish such frameworks with a legal basis under international law.<sup>xxxiii</sup>

### **The WHOIS database and public access policy**

Under the RAA, registrars are required to "provide an interactive web page and a port 43 WHOIS service providing free public query-based access to up-to-date data concerning all active Registered Names sponsored by Registrar in any gTLD."<sup>xxxiv</sup> The data accessible includes many different types of personal information, such as the name and the primary and secondary name server(s) and the contact details of the Registered Name, the identity of the registrar, the creation and expiry dates of the registration, and the name and postal address of the Registered Name Holder (3.3.1).

As others have said before,<sup>xxxv</sup> this obligation is incompatible with several international data protection instruments, which establish much higher standards for accessing and processing personal information by third parties. The WHOIS database system should not have unlimited public access to personal data, such as names, addresses, and e-mails. ICANN should ensure that it includes provisions governing the disclosure and third-party use of data consistent with international data protection principles<sup>xxxvi</sup>. Ideally, such provisions should provide that law enforcement officers be given access to personal information only subject to a valid court order.

## **ICANN must respect the right to privacy and data protection principles**

The above provisions are not only inconsistent with well-established data protection principles, they also have serious implications for the rights to privacy and freedom of expression. In particular, the publication of personal information on the WHOIS database may put human rights defenders or whistleblowers at risk in some countries. While private companies such as ICANN may legitimately be

required to provide personal information to law enforcement agencies, ICANN's current data retention policies in the RAA go beyond what is necessary under international data protection principles. This increases the risk that ICANN might be directly involved in human rights abuses.<sup>xxxvii</sup> This is consistent with the findings of the UN Human Rights Commissioner who said:

*'There may be legitimate reasons for a State to require that an information and communications technology company provide user data; however, when a company supplies data or user information to a State in response to a request that contravenes the right to privacy under international law, a company provides mass surveillance technology or equipment to States without adequate safeguards in place or where the information is otherwise used in violation of human rights, that company risks being complicit in or otherwise involved with human rights abuses.'*<sup>xxxviii</sup>

Accordingly, ICANN should provide stronger safeguards for the protection of personal data in order to act in the public interest in line with human rights standards. As a minimum, it should engage in meaningful consultation with affected stakeholders consistent with due diligence standards defined by the UN Guiding Principles. In the context of the RAA, this includes ensuring that domain name owners are provided with meaningful information about how their personal data is collected and potentially shared with others, so that they are able to raise concerns and make informed decisions.

## Conclusion

---

This paper seeks to highlight the need for ICANN to comply with due diligence so that it can protect the rights to freedom of expression and privacy. ICANN, as a globally operating non-profit corporation, with a leading role in the field of Internet governance, should both recognise its duty to protect human rights under the UN Guiding Principles and fully embrace it in compliance with human rights due diligence and its own Articles of Incorporation. In practice, this means transparency, accountability and meaningful consultation with affected stakeholders. In this sense, human rights provide an internationally agreed framework for checks and balances for the accountability system of ICANN. A human rights advisory council would guarantee consistency in discussions of issues relating to human rights and would provide more predictability in the policy making process. Moreover, it would ensure that ICANN acts consistently with human rights norms, which are an intrinsic part of its public interest role.

## Endnotes

---

<sup>i</sup> See Dr. Monika Zalnieriute and Thomas Schneider, 'A Council of Europe Analysis on ICANN's Procedures and Policies in the Light of Human Rights, Fundamental Freedoms and Democratic Values.' *Council of Europe*, Strasbourg, DGI (2014)12.

<sup>ii</sup> The UN 'Protect, Respect and Remedy' Framework for Business and Human Rights – UN Special Representative, Professor John Ruggie, endorsed by the United Nations Human Rights Council in June 2011. See the United Nations Human Rights Council, Guiding Principles on Business and Human Rights, HR/PUB/11/04, available at [http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf/](http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf/) (visited 12/01/2015).

<sup>iii</sup> On the relationship between freedom of expression and the gTLDs, see detailed expert report, Wolfgang Benedek, Joy Liddicoat and Nico van Eijk, 'Comments relating to freedom of expression and freedom of association with regard to new generic top level domains DG-I (2012)4, 12 October 2012, available at 15/01/2015) [http://www.coe.int/t/information/society/documents/DG-I%20\(2012\)%204%20FINAL%20pdf.pdf/\(visited](http://www.coe.int/t/information/society/documents/DG-I%20(2012)%204%20FINAL%20pdf.pdf/(visited)

<sup>iv</sup> The relationship between the so called 'expression function' of domain names and freedom of expression has been recognized among policymakers as well as judiciary: see, e.g., French Constitutional Council Décision n° 2010-45 QPC du 6 Octobre 2010, official translation into English is available at <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/201045QPCen201045qpc.pdf>, see § 6. See also, Cour d'Appel de Paris, Arrêt du 20 Avril 2003 Société Groupe Danone ct. Association Le Réseau Voltaire pour la liberté d'expression, p.12, available at <http://www.foruminternet.org/telechargement/documents/ca-par20030430.pdf>. This case concerned the usage of domain names [www.jeboycottedanone.com](http://www.jeboycottedanone.com) and [www.jeboycottedanone.net](http://www.jeboycottedanone.net); Dutch case of *Inholland vs. Kaasjager*, KG 05/447, 21 June 2005, available at [www.domjur.nl](http://www.domjur.nl); USA case of *Name.Space, Inc., v. Network Solutions, Inc. and National Science Foundation*, 202 F.3d 573, 577 (2d Cir. 2000), available at <http://www.yale.edu/lawweb/jbalkin/telecom/namespace.pdf>

<sup>v</sup> The right to privacy is enshrined in the Universal Declaration of Human Rights (UDHR), Article 12, and in the International Covenant on Civil and Political Rights (ICCPR), Article 17. The right to freedom of opinion and expression is enshrined in the UDHR, Article 19, and the ICCPR, Article 19.

<sup>vi</sup> The UN 'Protect, Respect and Remedy' Framework, p. 1; see also OECD (2011), OECD Guidelines for Multinational Enterprises, OECD Publishing. <http://dx.doi.org/10.1787/9789264115415-en/> (visited 20/01/2015).

<sup>vii</sup> Article 4 of the Articles of Incorporation reads as follows: "The Corporation shall operate for the benefit of the Internet community as a whole, carrying out its activities in conformity with relevant principles of international law and applicable international conventions and local law and, to the extent appropriate and consistent with these Articles and its Bylaws, through open and transparent processes that enable competition and open entry in Internet-related markets. To this effect, the Corporation shall cooperate as appropriate with relevant international organizations"

<sup>viii</sup> Sub-Commission on the Promotion and Protection of Human Rights, Commentary on the Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights, U.N. Doc. E/CN.4/Sub.2/2003/38/Rev.2 (2003), § 21.

---

<sup>ix</sup> The UN ‘Protect, Respect and Remedy’ Framework, p. 1.

<sup>x</sup> The UN ‘Protect, Respect and Remedy’ Framework, p. 13.

<sup>xi</sup> OECD Guidelines for Multinational Enterprises (2011 Edition), Commentary on Human Rights, Comment 38.

<sup>xii</sup> Benedek and Others, *op.cit.*.

<sup>xiii</sup> See GAC Communiqué – San Francisco, March 16, 2011, stating that “with the revised proposed ICANN ICM Registry agreement, the Corporation could be moving towards assuming an ongoing management and oversight role regarding Internet content” available at

[https://gacweb.icann.org/download/attachments/1540152/GAC\\_40\\_San\\_Francisco\\_Communique.pdf?version=1&modificationDate=1312225023000](https://gacweb.icann.org/download/attachments/1540152/GAC_40_San_Francisco_Communique.pdf?version=1&modificationDate=1312225023000); see also Applicant Guidebook, Module 3, section 3.5.3.

<sup>xiv</sup> See the new gTLDs Applicant Guidebook (the Guidebook), available at <http://newgtlds.icann.org/en/applicants/agb/> Module 2, section 2.2.1.2.3.

<sup>xv</sup> Module 2 section 2.2.1.3. The ICANN Board in explaining reasons for not following GAC advice regarding the potential risk/threat of TLD blocking to the universal resolvability and stability of the DNS stated that “[t]he issue of governments (or any other entity) blocking or filtering access to a specific TLD is not unique to the issue of the .XXX sTLD. Such blocking and filtering exists today. While we agree that blocking of TLDs is generally undesirable, if some blocking of the XXX sTLD does occur there’s no evidence the result will be different from the blocking that already occurs.” See 18 March 2011 ICANN Board Rationale for Approving Registry Agreement with ICM’s for XXX sTLD, Section V, 4, c, at page 16.

<sup>xvi</sup> The ICANN Board in explaining reasons for not following GAC advice regarding the potential risk/threat of TLD blocking to the universal resolvability and stability of the DNS stated that “[t]he issue of governments (or any other entity) blocking or filtering access to a specific TLD is not unique to the issue of the .XXX sTLD. Such blocking and filtering exists today. While we agree that blocking of TLDs is generally undesirable, if some blocking of the .XXX sTLD does occur there’s no evidence the result will be different from the blocking that already occurs.” See ICANN Board Rationale of 18 March 2011 for Approving Registry Agreement with ICM’s for .XXX sTLD, Section V, 4, c, p. 16.

<sup>xvii</sup> See ‘My ICANN’ website for this definition, available at <https://www.myicann.org/news/topics/1528/page/5/articles/14906?language=fr>.

<sup>xviii</sup> ICANN, Applicant Guidebook, Module 3 3-1 (2012) [Module 3; see *Objection and Dispute Resolution, ICANN*, <http://newgtlds.icann.org/en/program-status/objection-dispute-resolution> (visited 06/05/2014) (explicating the procedures for the four gTLD objections).

<sup>xix</sup> ICANN, Applicant Guidebook, Module 3, at 3-4.

<sup>xx</sup> ICANN, Applicant Guidebook, Module 3, at 3-4. The International Centre for Dispute Resolution (ICDR) handles string confusion objections.

<sup>xxi</sup> *Ibid.*

<sup>xxii</sup> ICANN, Applicant Guidebook, Module 3, at 3-4.

---

<sup>xxiii</sup> See generally ICANN, GTLD Applicant Guidebook Module 4, 4-1, 4-20 (2012).

<sup>xxiv</sup> *Ibid.* §4.1. The Applicant Guidebook mentions that all applications for identical gTLDs will automatically be placed in string contention proceedings and all similar gTLD applications will be evaluated by a String Similarity Panel to determine whether the gTLDs would create a probability of consumer confusion. *Ibid.* at 4-3.

<sup>xxv</sup> An auction will not take place to resolve contention in the case where the contending applications are for geographic names. See: Applicant Guidebook.

<sup>xxvi</sup> This is also acknowledged in the ICANN Applicant Guidebook, see Module 3, section 3.5.3.

<sup>xxvii</sup> UN Guidelines for the regulation of computerized personal data files, A/RES/45/95, 14 December 1990. Article 3(b): 'None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified.'

<sup>xxviii</sup> The revised OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data, 2013, available at <http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines/> (visited 12/06/2014). Article 9 of the OECD purports: 'The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.'

<sup>xxix</sup> International Standard on the Protection of Personal Data and Privacy, adopted at the 31<sup>st</sup> International Conference of Data Protection and Privacy Commissioners, 6<sup>th</sup> November, Madrid, 2009, available at [http://www.privacyconference2009.org/dpas\\_space/space\\_reserved/documentos\\_adoptados/common/2009\\_Madrid/estandares\\_resolucion\\_madrid\\_en.pdf/](http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf/). Article 7(2) reads: 'The responsible person should not carry out any processing that is non-compatible with the purposes for which personal data were collected, unless he has the unambiguous consent of the data subject.'

<sup>xxx</sup> Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981.

<sup>xxxi</sup> Asia-Pacific Economic Cooperation Privacy Framework of 2004. Principle III purports: 'The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.'

<sup>xxxii</sup> European Union 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 95/46/EC; OJ L 281, 23.11.1995, 31.

<sup>xxxiii</sup> The *Data Retention Directive* imposed data retention obligations on providers of public electronic communication networks and services, and registrars are not covered under this legislation. In any event, the Directive is declared invalid under the EU law.

<sup>xxxiv</sup> Section 3.3 of the Registrar Accreditation Agreement (RAA), <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en> (accessed 02/02/2015)

<sup>xxxv</sup> The Article 29 Party, Opinion 2/2003 on the application of the data protection principles to the Whois directories, adopted 13/06/2003, available at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp76\\_en.pdf/](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp76_en.pdf/) (visited 31/01/2015).

---

<sup>xxxvi</sup> See OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (2013), Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981, European Union 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 95/46/EC; OJ L 281, 23.11.1995, 31; Asia-Pacific Economic Cooperation Privacy Framework of 2004 among others..

<sup>xxxvii</sup> See UN 'Protect, Respect and Remedy' Framework, *op. cit.*

<sup>xxxviii</sup> See the report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/27/37, para. 43, available at [http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37\\_en.pdf/](http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf) (visited 15/09/2014).