Council of European National Top-Level Domain Registries

Report on ICANN64

Kobe
9-14 March 2019

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

Contents

Executive Summary 3

ccNSO report 4

Host presentation 4
Working Group and Committee updates 4
- TLD-Ops Standing Committee 4
- Auction proceeds WG 4
- Strategic and Operational Plan Committee (SOPC) 4

Policy Session 4
- PDP retirement WG 4
- WT5 update: Status 5

ccNSO Legal session 5
- NIC Chile database access request 5
- The Belgian Notice & Action charter 5
- Dealing with illegal content in Norway 6
- Legal issues affecting ccTLDs in Africa: Responses, actors and observations at regional and national levels 6

Other relevant ccNSO news: Internet Governance Liaison Committee 6

Other Relevant Sessions 7

Emerging Identifiers Technology 7
Domain Abuse Activity Reporting (DAAR) 7
Lessons learned: .dk shares their experiences on reducing abuse in their zone 7
Work of the Global Commission on Stability in Cyberspace 8

GAC report 9

General Data Protection Regulation and EPDP 9
- Phase 1 9
- Phase 2 9
- Further comments from the community on EPDP 10

Geographic names 11
Two-character codes at second level 12
DotAmazon 13
Challenges for ICANN in internet governance 14
- ICANN engagement with governments and standards bodies 14
- DNS over HTTPS 14

Executive Summary

ccNSO

The Kobe ccNSO meeting held few surprises. The Committees and Working Groups summarised their work from the last few months and the Policy updates showed that progress has been slow on the PDP retirement. The cross-community group discussing geographic names in future gTLDs is heading for a status quo, very close to the 2012 Applicant Guidebook. The PTI functions are running smoothly and the accountability mechanisms work well.

Despite this being a 'regular' ICANN meeting in the re-formatted meeting structure, this meeting was policy-heavy and process-focussed. To illustrate this: 75% of the time in the ccNSO members' meeting was spent on things happening within ICANN (processes, policy, working group updates, budget, strategy), while only 25% of the time was spent on things that happen in the ccTLD/DNS industry. Of those 25%, very few sessions covered new information.

The extension of the ccNSO Policy Development Process for the retirement and appeal policy from its initial two-year period to an additional three years is symptomatic of this 'process trumps substance' trend. Even if that new deadline is made, that means five (5!) years in total, absorbing thousands of extra working hours. It is important to note that the final document cannot be binding for ccTLD managers and therefore, any dispute will likely be dealt with in court anyway.

Some participants observed that this systemic obsession with process is paralysing the ICANN model to the level of dysfunctionality.

GAC

Link to the ICANN64 Kobe Communiqué

The GAC continued its extensive discussions on the on-going work of the EPDP and emphasised the need for ensuring appropriate access to WHOIS for third parties as a matter of priority. Other discussions included the on-going ICANN Board's disregard of previous GAC advice on two-character codes at second level, and the need to safeguard the regional interests of Amazonian countries within .amazon applications.

Other sessions

The ICANN Org has published its proposal for ICANN Organization Engagement with Governments and Standards Bodies that establishes the principles for the ICANN Org's engagement with decision-makers outside of ICANN when they are creating policy that impacts ICANN's ability to fulfill its mission. In essence, the proposal includes the monitoring of relevant initiatives and the intention to provide technical information to the stakeholders and decision-makers.

DNS over HTTPS was discussed in a few sessions and many believe that this should be a High-Interest topic for the next ICANN meeting.

The Domain Abuse Activity Reporting project (DAAR) illustrates the growing pressure on TLD managers to address and even prevent abuse.

ccNSO report

Host presentation

Hiro Hotta from .jp provided an interesting overview of this meeting's local host. JPRS has 1,552,763 domains under management, 600 RARs and 91 employees. There is a local presence requirement, and the .jprs gTLD is being run as a testbed and experimentation platform. Everyone is invited to send in ideas and suggestions for tests on this platform.

Working Group and Committee updates

TLD-Ops Standing Committee

- This group runs a contact repository of all ccTLDs, which proved its usefulness during a recent incident, where the list was used as the main channel to communicate that particular issue to other ccTLDs.
- The list currently has 380 contacts, covering more than 200 ccTLDs.
- The group is currently drafting a playbook, an effort which is being led by Dirk Jumpertz from EURid.
- As a reminder: early warnings of security risks are most welcome, so please circulate them on the list.

Auction proceeds WG

- This Working Group is tasked with designing mechanisms and processes to determine how the proceeds from gTLD auctions will be used. This WG does not decide which projects receive funding or not.
- Four mechanisms were proposed: internal deliberation by ICANN, internal deliberation by ICANN in cooperation with external charitable organisations, the creation of a new structure, or tasking an existing external organisation with taking care of fund allocation. Only the first three mechanisms are still being reconsidered.

Strategic and Operational Plan Committee (SOPC)

- ICANN is moving to a 2-year planning process; the main reason is that ICANN's planning department would be able to take on board comments more easily and to adjust the planning in light of those comments.
- The SOPC noted significant improvements to the 5-year plan:
  - More fiscal realism
  - More inclusion of community needs
  - More consistency against the strategic objectives
  - Still considerable differences in the narrative (missing KPIs).
- The ccNSO's comments on the Strategic plan 2021-2025 can be summarised as follows:
  - It includes a clear mission and vision
  - It has 5 relevant strategic objectives
  - It does a good job at prioritising work and balancing investments
  - There is a perceived overlap of certain goals
  - The targeted outcomes are not always easy to understand.

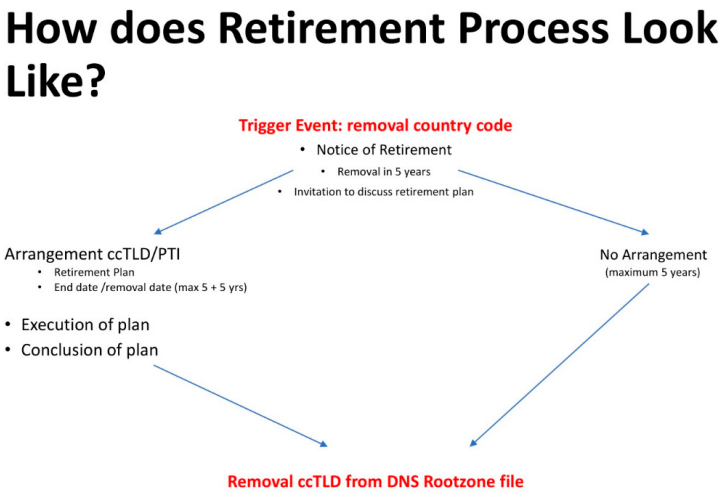
Policy Session

All presentations from the Policy Session can be found here.

PDP retirement WG

When the timeline for this PDP was announced in 2017, it was expected that it should have been finalised by January 2019. However, the reviewed timeline foresees the conclusion of the work by Q1 2022. An interim report is expected by October 2020.

- A graphic representation of the retirement process:



- The retirement plan is **voluntary** for ccTLDs. It aims to ensure the stability and interoperability of the DNS and an orderly and predictable retirement process for all stakeholders.
- A retirement plan is required to extend the duration from 5 to 10 years (this is the main incentive for ccTLD managers to cooperate).
- This plan is a guidance/policy for ICANN; it does not matter if the ccTLD is a member of the ccNSO or not.
- Next topics for the group to discuss:
  - Oversights of the retirement process
  - Exceptionally reserved country codes
  - IDN ccTLDs
  - Change of manager during the retirement process
  - Stress testing of the Policy
- The tentative deadline for completion of the work has been postponed until January 2022.

Relevance to ccTLDs

High. This PDP will eventually establish the process for retiring a ccTLD from the root zone. While it may not provide a legally binding policy, the process described in this document will give strong and detailed guidance as to how this will be accomplished.

WT5 update: Status

- There is general agreement in the group that the following names should remain blocked: all 2-letter combinations in the Latin alphabet
- There is agreement on the fact that country names should be banned, but disagreement remains as to whether or not they should be blocked in any language
- There is agreement on the need for governments or local authorities to support or refrain from objecting to:
  - Sub-national names (Wales)
  - Capital city names (Tokyo)
  - City names where the intention is to use it for that city's community. The difficulty here is that the trademark community rejects the need to support names that are also brands.
- There is strong disagreement on the Alpha-3 codes from ISO 3166-1. Should only 3-letter codes corresponding to an existing ISO3166 two-letter code be reserved, or should this include all 3 letter codes?
- This overview basically reflects the status back in 2012 as described in the Applicant Guidebook.

ccNSO Legal session

All presentations are available here.

NIC Chile database access request

NIC Chile received a request for a copy of the list of .cl domain names with the corresponding Tax ID of the registrant. They denied this request, and the claimant sued them before an administrative court.

Background: a few years ago, a request for a copy of their zone file was received by NIC Chile. In Chile, there is an obligation to inform registrants that their data is to be shared and they need to give their consent. This was done via email and 30k registrants replied that they did not consent. The requester withdrew their request, as did copycats, and similar requests were denied. At the end of 2018 a new request for the full list of domains was received, though this request did not ask for additional information such as the tax ID. NIC Chile refused, but following a complaint to the transparency council, they were forced to reconsider. The reasoning was that this request only asked for the domains. This is something registrants already agree to publishing anyway, but the registration agreement specifies that this is for the limited purpose of the management of the .cl registry and the operation of the DNS. Therefore, if published, this would violate the user agreement. NIC Chile filed an appeal at the court of appeals and if unsuccessful, they will go to the Supreme Court.

The Belgian Notice & Action charter

This is a new procedure that allows for fast action against fraudulent usages of .be domain names by overriding nameservers and putting in place a referral to a warning page of the Ministry of Economic Affairs. It has been formalised in a charter (including rights, obligations and guarantees) and does not replace existing procedures (Bad WHOIS policy, revoke procedure, request through subpoena). It is rather a last resort procedure and to be activated, all regular procedures must have been exhausted. This means that it is only to be used for cases related to a distortion of market equilibrium and if there is a clear and present threat to consumer protection.

This is a layered procedure and gives guarantees for DNS Belgium concerning its legal liability. If sued, the government will compensate the damages, though only if DNS Belgium executes the instructions properly. There have been 2 cases so far, affecting 115 domains in total. As had been expected, there has been no reaction from registrants so far. DNS Belgium is looking for similar arrangements with other stakeholders. The basic conditions are that they need to have the competence to assess the legality and the same liability safeguards for DNS Belgium.

Dealing with illegal content in Norway

The starting point for Norid's position on this issue is to stay away from content. Norid provides information and explains what happens when blocking or redirecting domain names and wants to ensure that everyone understands that tampering with the DNS is the last resort.

The logic behind this is that the domain holder should be the subject of a legal case, not Norid. This is because it is the domain name holder that 'creates' the domain through its registration. A Supreme Court decision from 2009 allows seizure the of domain names in criminal cases. This Supreme Court clearly stated that Norid does not have control for content. If they start an investigation, the law enforcement agency (LEA) takes on the registration, and if the seizure is lifted, the LEA must transfer the name back to its former holder? If the registration is forfeited, the LEA can keep it or sell it, though they will pay registration fees during that time. If the registration is deleted, there is a quarantine time of two years.

Legal issues affecting ccTLDs in Africa: responses, actors and observations at regional and national levels.

The African Union seeks to harmonise data privacy laws across Africa and Europe.

Many African countries have signed economic partnership agreements with Europe, and as such choose to comply with GDPR standards.

Trends in African ccTLDs:

- The majority of ccTLDs in Africa have legal expertise on their board of directors
- Few can afford an inhouse legal expert
- Smaller ccTLDs subcontract legal services, as there are fewer legal issues to deal with.

Common Legal issue

- Trademark infringement
- Dispute resolution
- Handling requests for Registrant information from LEA in order to solve Cybercrime-related challenges.

Observations:

- Putting ICT challenges in legal context is a problem
- Lack of knowledge
- Need for more legal expertise and capacity-building

Other relevant ccNSO news: Internet Governance Liaison Committee

Recently, the ccNSO Council approved the charter of the ccNSO Internet Governance Liaison Committee (IGLC). This group has been established to coordinate, facilitate and increase the participation of ccTLD managers in Internet Governance-related discussions and processes. The scope is limited to:

1. Providing input to the ccNSO and share information on issues pertaining to Internet Governance discussions, events and processes.
2. Ensuring that such input as mentioned above is reflected in the ccNSO's activities in discussions and processes pertaining to Internet Governance. The ccNSO is currently looking for volunteers to join the Committee.

More information can be found here.

Relevance for ccTLDs

Low. This is a ccNSO internal liaison committee.

Other Relevant Sessions

Emerging Identifiers Technology

Both presentations are available here.

ICANN's Paul Hoffman provided an overview of DNS technologies over secure transports: DNS over TLD (DoT) and DNS over HTTPS (DoH). The swift implementation of the DoH RFC took the community off guard. Plenty of policy questions need to be addressed and participants in this session would like to see a broader debate taking place in ICANN on these issues. It will only be possible to make a proper impact assessment of the impact of DoH on the DNS ecosystem if and when browser companies and resolvers start providing clear answers on user choice. According to Paul, Mozilla has confirmed that they will develop a program to get 'accredited' as a trusted resolver. The user will have a choice on which resolver they prefer.

Relevance for ccTLDs

High. See also the coverage of this topic in the GAC. While the technical aspects are uncontroversial, the policy implications could have far-reaching consequences for the DNS industry and have been largely unexplored.

W3C's Wendy Seltzer presented on Decentralised IDs (DIDs). DIDs have structured formats that look like: [did:did method:did method identifier] -> [did:btcr:xkyt-fzgq-qq87-xnhn]

Domain Abuse Activity Reporting (DAAR)

The DAAR project is an ICANN initiative that aims to develop a system for reporting on domain registration and abuse data across TLD registries and registrars. It allows for historical research, studies multiple threats (such as malware, phishing and spam) and for now studies all gTLD registries and registrars whose zone file and registration data are collected. DAAR should allow for more informed security decision-making and policy.

Some participants (Tucows Inc., Verisign) warned that ICANN should stay away from content, and that this exercise was bordering on assessing the content of a website. ICANN responded that they are very selective in their choice of data feeds (particularly in terms of staying away from website content).

Other concerns expressed were that non-existing (deleted) domains still show up in the reputation feeds. This means that registries that take action to address reported abuse still see a negative impact on their reputation, even after the problem has been addressed.

(Earlier discussions in the CENTR Security Working Group on this topic mainly focussed on the governance models for the different providers of abuse models, transparency and appeal procedures.) ICANN confirmed that the governance model of the abuse feeds is indeed an important decision factor, whether they are included in DAAR or not.

There was no clear answer on how one can make the distinction between compromised versus malicious domains.

The (excellent) presentation is available here.

Relevance for ccTLDs

High. DAAR will add to the pre-existing pressure on TLDs to address and even prevent abuse.

Lessons learned: .dk shares their experiences on reducing abuse in their zone

DK Hostmaster shared their insights into the measures that have been implemented to reduce the number of abusive domains in the .dk zone. Jakob Bring Truelsen shared DK Hostmaster's experience with cleaning up the .dk zone, which has an open registration policy that is not limited to Danish citizenship or residence.

Denmark's legislative instrument "Domain Act" predates the GDPR. According to national law, the WHOIS must be publicly available. As such, the aforementioned piece of national legislation automatically provides a legitimate purpose for data processing under the GDPR ("public interest" exception in Article 6). The aforementioned national precedent of publicly available WHOIS has also been

approved by the local Data Protection Authorities (DPAs), that confirmed the Domain Act's compliance with the GDPR. During the session, Europol praised the positive example of .dk and the importance of the Domain Act and publicly available WHOIS for fighting abuse online.

In order to ensure the accuracy of information in the WHOIS and to identify abusive registrations in a timely manner, .dk has established a system to verify registrants' identity by using the national eID system for Danish nationals, and by requiring identifying documentation from foreign registrants (e.g. ID cards, passports, driver licences and selfies). There is an automatic risk assessment system that was developed in-house that scores all registrations from "low" to "high" risk. Jakob Bring Truelsen stressed that the registry does not look into the content of websites, as it considers content-scanning to be inconsistent with the role of a registry as a provider of technical infrastructure. Nor does the registry act upon notifications from rightsholders, who can only enforce their rights in court. Jakob Bring Truelsen added that there is a substantial interest for the registry to have such a system in place, despite the cost. The registry is acting in the public interest and is not just a commercial player that is solely interested in profits. DK Hostmaster is committed to maintaining a safe and trustworthy domain zone.

Work of the Global Commission on Stability in Cyberspace

The Global Commission on Stability in Cyberspace (GCSC) presented its on-going work, that comprises of the 8 norms that are responsible for ensuring the safety and stability of cyberspace, without stifling digital innovation. The norms target both state and non-state actors to, inter alia, protect the "public core of the internet", including internet routing, the domain name system, certificates and trust, and communications cables. The full recording of the presentation by the GCSC at the meeting with the ICANN At-Large Advisory Committee is available here.

GAC report

General Data Protection Regulation and EPDP

On 17 May 2018, the ICANN Board adopted the Temporary Specification for gTLD Registration Data (hereinafter Temp Spec) as a temporary policy in response to the EU General Data Protection Regulation (GDPR) taking full effect on 25 May 2018. The Temp Spec was intended as a temporary policy with an expiry date of 1 year. As a consequence, on 19 July 2018, a GNSO Expedited Policy Development Process (EPDP) was initiated to replace the Temp Spec before its expiration in May 2019. GAC representatives from the European Commission, India, Iran, the UK and the US participated in the substantial discussions of the EPDP Team that can be summed up in 44 conference calls, 3 multi-day face-to-face meetings and 1600+ emails. As a result of the work of the EPDP Team, on 4 March 2019, the GNSO Council adopted the EPDP Final Report after the conclusion of Phase 1 of the EPDP. The Final Report needs to be voted on by the ICANN Board at some point before 25 May 2019 and after a round of public consultation. The public can comment for 42 days starting from the adoption of the Final Report on 4 March by the GNSO Council. The effective date for the new policy needs to be confirmed by 29 February 2020. The conclusion of Phase 1 immediately set in motion the formation of an implementation review team and the initiation of Phase 2 of the EPDP, as several critical questions that emerged in the course of the work the EPDP Team still require answers.

In the GAC Communiqué from Barcelona (25 October 2018), it was noted that the Temp Spec fails to meet the needs of law enforcement, cybersecurity researchers and IP rightsholders. To reiterate previous developments and the division of work within the EPDP Team, the importance to ensure third-party access to WHOIS data was not dealt with in Phase 1. In addition, the GAC's general concern with the Draft Final Report was that it does not sufficiently recognise the benefits of the WHOIS database. Other issues flagged by the GAC were to request a legal review to ensure that previous guidance from the EDPB and WP29 are taken into account and that Phase 2 is started as quickly as possible.

Phase 1

The European Commission highlighted the discussion about accuracy of WHOIS data that has not been addressed by the Final Report. The GAC believes that data accuracy is essential for serving all data-processing purposes, not only in relation to registrant's rights but also for third party access to this information, and for the public interest in general.

The issue of the distinction between legal and natural persons was subject to heated debates within the EPDP Team and became controversial. There was a recommendation to pursue a further study to conclude these discussions and to take into account the feasibility and costs associated with this distinction, examples of companies and organisations that do already make that distinction, as well as privacy risks for individuals. Recommendation 17 of the Final Report concludes that the EPDP Team will discuss this issue further in Phase 2.

Recommendation 18 deals with the question of the "Reasonable Requests Lawful Disclosure" criteria. This is the point about access to non-public registration data for third parties that the GAC has been pushing for in relation to the Temp Spec. The so-called Unified Access Model was out of the scope in Phase 1, however, Recommendation 18 of the Final Report recognises the potential of a "Standardized Access to Non-Public Registration Data" system to complement, revise or supersede the requirements set in Recommendation 18. While according to some GAC members (like the US), Recommendation 18 does not provide much clarity for third party access requests, it nevertheless sets some expectations on the contracted parties to respond to such requests. For example, the time for "reasonable" response to data access request is bound to acknowledging the request in 2 days, while resolving such a request should be done in 30 days.

Phase 2

In parallel with the EPDP, the ICANN Org has been conducting work on the Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data (i.e. Unified Access Model). This work is conducted outside of the scope of EPDP. In

Barcelona, the ICANN Org set up a Technical Study Group For Access to Non-Public Registration Data (TSG), which is reviewing aspects of the possible Unified Access Model from a technical perspective. On 7 March, the Technical Study Group revealed its Draft Technical Model for Access to Non-Public Registration Data, which is based on the technology available via the Registration Data Access Protocol (RDAP). The purpose of the TSG is to explore technical solutions for authenticating, authorising, and providing access to non-public registration data for third parties, with the intent to reduce the potential liability faced by gTLD registries and registrars when providing such access under the GDPR. The TSG is not equipped to solve any policy questions, nor to give recommendations on who gets access, which data fields are covered, which conditions should access be given under, what is a legitimate interest, etc. The Final Technical Model is expected to be published on 23 April 2019.

During the Community Engagement session on the work of the TSG, the members of the group stressed that their work does not provide definite answers on whether the proposed technical model will in fact reduce potential liability under the GDPR. The TSG recommends that the contracted parties make up their own minds about this point, based on their own legal advice.

The GAC's priorities for Phase 2, and particularly in regard to the Unified Access Model, are to come up with a clearly defined and definite timeframe to deliver on the remaining questions expeditiously; to clearly define the narrow scope of Phase 2, and to have sound legal advice upfront and throughout. The GAC continues to consider that the ability for third parties with legitimate interests to access non-public registration information is of critical importance and as such, must be treated with the same amount of urgency as Phase 1 activities. Without the clear timeline as was the case in Phase 1, it is unclear whether any of the questions deferred to Phase 2 will be dealt with as speedily as in Phase 1.

Further comments from the community on EPDP

- During the Cross-Community session on GDPR, Goran Marby stated that the technical study is only one part of the solution. According to Marby, on top of the study, ICANN needs to look into third party accreditation houses (e.g. WIPO, Europol) that might provide some framework on the possibility of such an accreditation system. He also called for the European GAC representatives to share their experiences of GDPR implementation with the ICANN Org.
- Ashley Heineman from the US government highlighted that it is not clear whether the accreditation system is something that ICANN should look into, or whether this should be left for the third parties to figure out.
- Cathrin Bauer-Bulst from the European Commission highlighted the need to ensure the accreditation, authenticity, access and accountability within the EPDP process, as these are important from a public safety perspective. She also added that there is little guidance from data protection authorities (DPAs) on the questions in Phase 2 because the DPAs were mostly concerned about the amount of personal data being publicly available. However, for Phase 2 the necessary guidance can be derived from existing case-law that verifies that WHOIS data is not particularly sensitive.
- Stephanie Perrin from the Non-Commercial Stakeholder Group (GNSO Council) pointed out that in her view, ICANN should not be managing the issue of access, but that it should instead be maintained by other independent entities. ICANN's role is to ensure the fair, competitive and neutral operation of the DNS, rather than dealing with political questions like access.
- Elliot Noss from Tucows pointed out that the number of data access requests after the entry into force of the GDPR has been very low. The problem with cybersecurity needs in data access is that registrars do not have engineering skills to pseudo-anonymise the data. According to Noss, the cybersecurity community could take care of a third-party solution that is open for registrars to use.
- The Public Safety Working Group mentioned that, according to the figures accessible to them, the unavailability of WHOIS data has been dramatic for the LEA. There have been delays in 52% of investigations because the data is no longer available. 26% of investigations are being dropped completely, which has a serious impact on public safety.

- Cathrin Bauer-Bulst from the European Commission stated that there is a need to ensure confidentiality in law enforcement data access requests and the reverse look-up of WHOIS data to identify abuse patterns. According to the TSG, the RDAP currently does not support reverse WHOIS searches, however, there are discussions at IETF level that would enable this.

GAC Communiqué: the GAC consensus advice to the ICANN Board is to take the necessary steps to ensure that the EPDP institutes concrete milestones, progress reports and an expeditious timeline, similarly to Phase 1, in order to conclude the Phase 2 activities. This implies taking the necessary steps to ensure that the scope of Phase 2 is clearly defined with a view to its expeditious conclusion and implementation; to consider instituting additional parallel work efforts on technical implementations, such as that carried out by the Technical Study Group, for the purpose of informing and complementing the EPDP's Phase 2 activities.

Relevance to ccTLDs

The EPDP does not make any policy recommendations developed by ICANN that are binding for ccTLDs. The policies governing ccTLDs are deeply rooted within their local jurisdictions and based on the needs of local internet communities. Nevertheless, whichever GDPR implementation ICANN adopts could affect ccTLDs indirectly, as in addition to gTLDs, registrars are also bound by the ICANN policies. Individual ccTLDs' experiences with GDPR implementation can also give guidance to the on-going work in the EPDP. Since the adoption of the Temp Spec, several ccTLDs have been in the spotlight, sharing their experience of GDPR compliance with the ICANN community.

Geographic names

Work Track 5 (WT5) is a sub-team of the New gTLD Subsequent Procedures Policy Development Process (PDP) Working Group (WG). The overall WG is tasked with determining whether and which changes are needed to the existing 2007 Introduction of New Generic Top-Level Domains policy recommendations. WT5 seeks to review the existing policy and implementation related to the topic of geographic names at the top level, determining if changes are needed and recommending revised or new policy and/or implementation guidance. WT5's scope includes questions that concern geographic names at the top level, including two-character ASCII letter-letter combinations at top level, country and territory names (incl. alpha-3), capital city names, sub-national names (e.g. county, province, state etc), UNESCO-protected regions, and other geographic names (e.g. rivers, mountains etc) and culturally significant terms related to geography.

On 5 December 2018, WT5 published its first Supplemental Initial Report that was open for public comments. By the end of the public consultation period, 42 comments had been received in total. Respondents included both governments and individual ccTLD managers. The comments received have been compiled into a Public Comment Review Tool, colour-coded to see where agreements have been reached, and where more discussions are needed. As a result of the partial assessment of the public comments, it was concluded that the majority of comments support the continuation of the 2012 implementation (so-called "Applicant Guidebook"), with the exception of the intended use provision assigned to non-capital city names. In addition, concerns were raised about the basis for preventive protection beyond the 2012 implementation.

WT5 continues to meet and review the remaining issues in public comments. Several proposals for community input still need to be reviewed.

Relevance to ccTLDs

For ccTLDs, Preliminary Recommendation 2, that suggests "continuing to reserve all two-character letter-letter ASCII combinations at the top level for existing and future country codes", is of particular importance. This is where the issue of allowing 1-letter/1-digit strings was raised in the public consultation round, as there is a risk of similarity between existing country-codes and confusingly similar new combinations (e.g. .f1 and .fi, or .n1 and .nl etc). WT5 has determined this issue to be out of scope, due to the fact that these combinations are not geographic names. It is yet to be decided whether the issue of 1-letter/1-digit strings can be moved to WT2 instead. WT2 is referenced in this regard because some considerations of the application process look at string confusion. As a result, 1-letter/1-digit combinations might be put through a confusion test instead, rather than being completely restricted. Discussions

included the call for clarifications in connection to the "similarity standard" that is currently being developed and the issue of 1-letter/1-digit strings being confusingly similar to ccTLDs. It was outlined that a consistent standard on similarity needs to be applied throughout.

Other divergent issues that are relevant for ccTLDs also included the question of alpha-3 codes in the ISO-3166-1 standard, that should be made available for registration. Some participants support the general availability to any applicant, whilst others only with the approval with the government or public authority. During the meeting, the right of a country to its country code was questioned. However, participants were reminded that whatever conclusion the WT5 comes to, this would mean little for ccTLDs in practice. No cross-jurisdictional rule can be established as a result of a work of WT5, as each country can overrule these practices with a respective court ruling. This is exemplified by the "france.com" case, where the state of France successfully claimed the country's sovereign right to the word "France", and demanded that the privately-owned domain name france.com be transferred to the French Republic as a result.

GAC Communiqué: The GAC recalls its advice in the ICANN56 Helsinki Communiqué, which states that the development of policy on further releases of new gTLDs needs to fully consider all the results of the relevant reviews and analysis to determine which aspects and elements need adjustment. The GAC advised the Board to address and consider these results and concerns before proceeding to a new round.

Two-character codes at second level

The current situation regarding the use and release of two-character country codes at the second level allows for the registration and use of country codes at the second level without needing to obtain prior authorisation or notification of the relevant ccTLD or the government. The GAC remains concerned by the fact that the current situation with two-character codes at the second level is a result of a blanket authorisation by the ICANN Board, on the condition that TLD operators were to adopt certain matters to avoid confusion with the corresponding ccTLD.

During ICANN63 in Barcelona, the GAC discussed the Briefing memo, that was prepared on this matter and that identifies a number of issues with the current process concerning two-character codes at the second level. According to the ICANN63 Briefing, concerned countries are wary of the fact that countries lose the ability to play any role in the release procedure. Other concerns identified in the Briefing include the ICANN Board's dissatisfactory explanation for the changes and the inability to adopt measures to prevent further consequences for the concerned GAC members. Furthermore, the GAC considers that there have been serious procedural flaws in the decision-making process. In particular, the fact that the ICANN Board adopted a decision that significantly affects the process recommended under GAC advice before considering and responding to the respective GAC advice, and without prior consultation with the GAC.

The Briefing was submitted to the ICANN Board for consideration and the GAC advice from Barcelona urged the ICANN Board to explain how the process that led to the retirement of the authorisation process was consistent with previous GAC advice.

On 22 January 2019, the ICANN Org released a Memo on the Implementation of the Release Procedure and an Historical Overview of Events. On 27 January 2019, the ICANN Board addressed the GAC Advice in its resolution. In its memo, the ICANN Board disagrees with the concerned GAC members on the fact that the release of the two-character codes at the second level is inconsistent with the previous GAC advice and considers these concerns not to be substantiated enough.

The GAC seeks to identify whether any of the procedural and substantive concerns have been addressed by the recent developments. The discussions within the GAC highlighted the fact that substantive concerns should be prioritised and questioned whether the new tool introduced by the ICANN Org, allowing members to check if the two-character code is used, will help mitigate the risk of confusion when the two-character code is used at the second level. During the meeting with the ICANN Board, the GAC expressed their appreciation for the development of the two-character tool, which may address the concerns of some GAC members related to the risk of confusion created by the use of country-codes at the second level. The GAC has agreed to use the Montreal meeting to check base, once the tool has been used for some time.

GAC Communiqué: The GAC appreciates the development of the two-character tool, which may address the concerns of some GAC members related to the risk of confusion created by the use of country-codes at the second level under new gTLDs. GAC members will try using the tool over the coming period and have agreed to have the Montreal meeting as a checkpoint.

Relevance to ccTLDs

Some countries remain possessive over the use of their country codes at the second level. The issue continues to remain procedural, as the GAC considers that there has been no sufficient response from the ICANN Board yet on why the GAC consensus advice was rejected without any further explanation. The ICANN Board seems to have a diverging view on the interpretation of the previous GAC advice, illustrating tensions between governments and the ICANN Org in the multistakeholder governance model.

DotAmazon

The Brazilian Ambassador presented a summary of the on-going .amazon application process, requested by the US company Amazon Inc. In 2017, the GAC advice to the ICANN Board was to find a mutually acceptable solution to the .amazon application. The rationale of that GAC advice was to reconcile the concerns of Amazonian countries, while allowing the use of .amazon as a top-level domain name.

In September 2018, the Amazonian countries indicated in their letter to the ICANN Board that they were willing to accept a solution for the delegation of .amazon with a shared governance after discussing the possible model for such shared governance with the ICANN CEO. During ICANN63, the ICANN Board adopted a resolution that stopped the process of dialogue for a mutually acceptable solution, as according to the Brazilian Ambassador, it was "badly-worded".

ICANN CEO Goran Marby reiterated that the current GAC advice on the matter is for the ICANN Board to facilitate discussions between the parties concerned. The ICANN Board resolution in question was made in line with these discussions and mandated the ICANN CEO to have a final discussion with the concerned Amazonian countries. According to Marby, he has attempted to meet with the countries concerned twice since the adopted resolution, however both meetings were cancelled. He pointed out that Amazon Inc., on the contrary, has been very helpful in the on-going discussions.

The US refused to recognise any inherent governmental right to geographic names. The US representative expressed their lack of support for any further GAC advice on the issue of .amazon applications. Furthermore, according to the US, this is no longer a GAC issue, and Amazonian countries should continue their dialogue directly with Amazon Inc. in order to be able to find ways to address their concerns. The GAC's involvement on this matter is no longer necessary, according to the US representative.

Colombia, on the other hand, expressed their duty to protect the cultural, social, economic and environmental rights of an area that is highly sensitive for the whole world. Colombia called for the attention of the GAC to this issue in order to maintain the perspective and the vision of multistakeholderism.

Switzerland, France and the European Commission called for the continuation of discussions within the ICANN environment in order to find a mutually acceptable solution. Switzerland proposed the introduction of a clear timeline to be able to frame these discussions in a timely manner, and to make sure that a mutually acceptable solution is found.

During the GAC's meeting with the ICANN Board, Brazil and Colombia both made statements reflecting the need to safeguard public interest and to enable the Amazonian countries to participate in the management and use of .amazon applications, with the aim to protect and promote the natural, cultural and ethnic heritage of the Amazon region. Brazil expressed its hope for Amazon Inc. to pay attention to the sensitivity and the public interest involved.

Relevance to ccTLDs

There seems to be some fatigue with the .amazon applications discussion expressed by some GAC members who are no longer interested in having these discussions in the GAC. These members believe that this is now solely a regional issue, that needs to be solved bilaterally between the concerned countries and the Amazon company. The countries' right to their online legacy does however remain a topic that is also consuming the

time of WT5 on geonames, as the .amazon case is at the forefront of cultural sensitivity not only for countries but also for non-sovereign regions. The .amazon case also illustrates the highly political nature of these discussions.

The ICANN Org reaction to the regional concerns may give an interesting glimpse into how it may be handling its intended further engagement with politicians to "educate" the latter on technical topics (see next section on "Challenges for ICANN in internet governance" for further information). After all, the GAC represents the same governments that ICANN wishes to "educate" further on. The .amazon application case is an illustration of the difficulties that multistakeholder fora like ICANN face when trying to safeguard the interests of its community, a community that consists of stakeholders with conflicting stakes.

Challenges for ICANN in internet governance

ICANN engagement with governments and standards bodies

Several references towards the enhanced cooperation towards of ICANN with the governments were made during ICANN64.

In light of the increased legislative pressure on operators of the internet infrastructure, on 25 February, the ICANN Org published its proposal for ICANN Organization Engagement with Governments and Standards Bodies. This proposal establishes the principles for the ICANN Org's engagement with decision-makers when a government or non-Internet-related standards body is considering a proposal that impacts ICANN's ability to fulfill its mission. Examples of this impact could include (1) the security, stability, resiliency or interoperability of the Internet's unique identifier systems; or (2) existing ICANN consensus policy. The proposed principles limit the ICANN Org's engagement with legislative proposal to providing technical information; the ICANN Org will maintain a publicly-available list of proposals for which the ICANN Org intends to or is considering engagement; and in case the ICANN Org provides any written comment on the proposal, this comment will be available on the ICANN Org website.

During the meeting with the ICANN Board, Goran Marby addressed the GAC audience by highlighting the increased legislative pressure on the internet infrastructure to address the challenges that unwanted content is posing online: e.g. "fake news". According to Marby, ICANN has not been very efficient in explaining the difference between people connecting to the internet and the applications and platforms on top of the internet that pose policy challenges. Therefore, ICANN proposed the aforementioned document in order to find ways to explain to the legislators if and when their proposed legislative proposals can "actually break the internet" or fragmentise it as a result. In addition to legislative proposals, there are also other proposals that fall in the technology remit, that could have an effect on the way people connect to the internet. For instance, 5G is one of such proposals that has recently been getting traction. However, according to Marby, the on-going 5G discussions also include the calls for using alternative identifier systems, that in essence also means creating an alternative internet.

ICANN is, therefore, hoping to mitigate these unintended consequences where possible by "providing accurate factual technical information that addresses any misconceptions about how the Internet actually works".

DNS over HTTPS

The challenges that some of the on-going standardisation proposals within the technical community pose to the internet infrastructure and ultimately for internet governance as a multistakeholder model, has also been highlighted during the GAC meeting with the ccNSO. During this session, Peter Van Roste (CENTR) gave a presentation about the on-going standardisation efforts within the browser community to mitigate internet users' privacy and security concerns. In particular, the IETF has already published an RFC on "DNS over HTTPS" (hereinafter DoH). The new standard in question intends to encrypt all DNS traffic and to eliminate all man-in-the-middle attacks as a result. The technical solution to this type of privacy-enhanced measure is however to resolve all DNS queries through a "trusted" third-party provider, instead of a local ISP. The "trusted" resolver will be a hard-coded choice by the browser. While the technical solution seems to be plausible for enhanced user-privacy, it completely disregards any policy implications that such a technical solution may pose to the current decentralised nature of the internet.

There is not only a limited number of browsers, but also a limited number of third-party providers that can both handle the amount of DNS queries in the new set up and have acceptable data processing policies for browsers. As a result, the resources will be consolidated naturally to a handful of big players that are residing in a few jurisdictions (mainly the US). It is unclear how those jurisdictions will serve the needs of the global internet community, both from the perspective of judicial authorities (i.e. a European court order for a respondent based in the US?), as well as from the user experience (will an individual using Chrome see the same content in Firefox?). Finally, what will ICANN's role be in a set up where a handful of players can decide which domain names to resolve or not? Answers to many policy questions are currently pending.

There was a legitimate question from the audience regarding the inquiry of possible ICANN responses to the challenges posed by DoH and which steps ICANN could take. Peter Van Roste highlighted that present discussions within ICANN stay primarily within the technical community. However, there is a need for a broader discussion on DoH within the whole ICANN community. Peter Van Roste suggested including DoH as a high-interest topic for following ICANN meetings.

Relevance to ccTLDs

Increased legislative pressure on operators of the internet infrastructure in the layers other than applications is a recognised trend. In addition to the increased regulatory attention, the policy-making that affects the foundation of the internet as we know it today is also happening on transnational level in different fora, including standard-setting bodies. As a result, one can observe a so-called forum-shopping in policy development processes, where particular policy goals are pursued within different fora in order to achieve the desired outcome, either by legislation or technical implementation. Either way, ccTLDs could be significantly impacted if the changes mean that the current identifier system is completely changed, or the existing authority of the root is abolished. It is, therefore, a necessity for the whole ICANN community to stay on top of these developments and to ensure that the multistakeholder model of internet governance is respected.

ICANN65 will be held on 24-27 June 2019 in Marrakech, Morocco.

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 55 full and 9 associate members – together, they are responsible for over 80% of all registered domain names worldwide. The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD registries.

Rate this CENTR Report on ICANN64

(Thank you for your feedback!)

CENTR vzw/asbl
Belliardstraat 20 (6th floor)
1040 Brussels, Belgium
Tel: +32 2 627 5550
Fax: +32 2 627 5559
secretariat@centr.org
www.centr.org

To keep up-to-date with CENTR activities and reports, follow us on Twitter, Facebook or LinkedIn