Regulating the domain name system: approaches to ccTLD policies internationally

Table of Contents

Introduction

The .nz policy review

InternetNZ is undertaking a review of the .nz policies which set out the rules and procedures for registering and using a .nz domain name. The review will make sure .nz is modern, robust, safe and world-class.

We have appointed the .nz Advisory Panel ('the Panel') to help us review the policies related to the .nz domain. The Panel are exploring a wide range of important issues and ways we might solve them together.

This paper is a contribution to InternetNZ's .nz Policy review. Its primary audience is the .nz Advisory Panel, but we are also releasing this research publicly so everyone can benefit from it.

Why we conducted this research

The Panel has recently released its Issues Report, and it is currently developing policy options for the issues identified. We wanted to embed this work in an international context, and see how other ccTLD operators are tackling these big issues. The Panel may look to these other ccTLDs to learn from their experiences and make the best recommendations for New Zealand's domain name system.

This paper looks at six other ccTLDs:

1. .se, Sweden's ccTLD managed by the Swedish Internet Foundation
2. .de, Germany's ccTLD managed by DENIC
3. .nl , the Netherlands ccTLD managed by SIDN
4. .dk, Denmark's ccTLD managed by DK Hostmaster; the registry for DIFO (the Danish Internet Foundation)
5. .jp, Japan's ccTLD managed by JPRS
6. .za, South Africa's ccTLD managedby ZADNA.

We wanted to know how their ccTLD policies covered key issues facing .nz, including:

- What are the guiding principles that inform how a ccTLD is managed?
- How do registrants, registrars, resellers and the registry interact with each other?
- How do registries protect the privacy of registrants?
- How is the notion of first come first served operationalised?
- Do ccTLDs have prohibited domain names, or registration restrictions?
- How are human rights protected and promoted in the management of the ccTLD

- How does the management of the ccTLD promote the growth of the domain name space, growth of the businesses using domain names, and protect consumers?
- Do ccTLD's have local presence or geographical requirements for registration? How is this enforced?
- Do ccTLD's regulate website content associated with their domain names?
- How is security of the domain name space, and all of the actors within it, promoted in the management of the ccTLD?

Limitations of this paper

This project was conducted as desk-top research, and the information in this paper is all publicly available, as the ccTLD managers have reported it. Due to these conditions, there may be:

- information gaps where it could not be found, context missing about why the ccTLDs are run a certain way, and
- written policies that may differ with the way they are implemented or
- actioned.
- We have verified the accuracy of this paper to the best of our ability, and welcome any comment or correction.

How to use this paper

This is a neutral summary of policies of the six ccTLDs on the areas we have listed above. The paper provides different ways ccTLD managers have prioritised and approached issues, but does not analyse the context in which the policies were implemented, or the impacts of these policies on the domain name system, or give advice on how to incorporate into the Panel's thinking and analysis to develop options.

Principles

What are the common overarching principles that guide ccTLD policies?

Overview

It was found that there is a diversity of overarching principles among the ccTLDs, from comprehensive code of conducts for employees to "general" mission statements and principles. Some are elaborate, others are brief. While there is no one particular model, their importance to shaping the purpose and mission of the ccTLDs is without question.

The range is encapsulated by, on the one hand, .se ccTLD which has both a comprehensive mission statement and a code of conduct. The latter focuses on employee responsibilities and notes, for example, the importance undertaking activities in line with international human rights conventions.

On the other hand .za ccTLD has few "principles" focussing rather on the powers derived from the mandate provided by the South African government. There are no particular overarching principles similar to those discussed below.

The principles articulated by the six ccTLDs can be broken down as follows:

- General operating principles related to security, functioning of the ccTLD, etc.
- General principles relating to non-technical issues such as consumer interests, human rights, growth, etc.
- Principles that relate to ccTLD management and personnel behaviour
- And, principles that are embraced as a part of the broader Internet ecosystem, and particularly as they relate to Internet Governance and associated characteristics of openness, multi-stakeholder approaches, etc.

Some ccTLDs have explicit "mission" statements and/or clear principles; others state their "purposes" in their "About" Pages. All are included below to give the fullest sense of the breadth of the principles embraced by the six ccTLDs.

Are there principles that tend to be common to most ccTLDs?

Most ccTLD mission statements and sets of principles focus on three key issues, as outlined further below:

1. Security, including maintaining and contributing to Internet infrastructure

2. The development of the Internet and its future; and

3. A focus on the consumer and the general need to be responsive to consumer interests and demands so as to enable them to fully enjoy the Internet.

Security:

Security is the most common principle cited in the various ccTLD vision/mission statements.

The Swedish Internet Foundation's code of conduct refers to maintaining the "highest possible technical and organizational security level in order to protect critical operations as well as sensitive and personal information."[1] Its Charter states that "we shall ensure a strong and secure infrastructure for the internet in Sweden…".

SIDN's (Netherlands) vision statement asserts: "it's vital that people can be confident in the internet's quality, security and privacy." Its mission "… is connecting people and organisations to promote safe and convenient digital living. We seek to do that by keeping the .nl domain as stable and secure as possible…".[2]

The "About DENIC" (of Germany's registry, .de Network Information Centre) website page states that "Our entire infrastructure, our technical processes and internal procedures are all geared towards security."[3]

Although JPRS (Japan) does not refer specifically to security, it references the importance of reliability and stability in its Corporate Profile which are framed as elements in the broader notion of security.[4]

DK Hostmaster, the registry arm of the Danish Internet Forum (DIFO) states in its "About page" that "Our aim is to provide stable and reliable operations as well as the highest level of security and service…".[5]

Development/evolution of the Internet:

JPRS, from its Mission (from the Corporate Profile): "As a company dedicated to maintaining the Internet infrastructure of Japan, Japan Registry Services (JPRS) contributes to the development of the Internet and the building of a better future for everyone." It continues to state that "in the interest of both the global community

[1] https://internetstiftelsen.se/en/we-are-the-swedish-internet-foundation/code-of-conduct/
[2] https://www.sidn.nl/en/about-sidn/what-we-stand-for
[3] https://www.denic.de/en/about-denic/
[4] https://jprs.co.jp/en/about/jprs-profile_en.pdf
[5] https://www.dk-hostmaster.dk/en/dk-hostmaster

and the community in Japan, JPRS is developing, improving, and promoting its services to ensure that .JP domain names are more user-friendly and have higher value."

The Swedish Internet Foundation's Introduction and Charter: "The Swedish Internet Foundation is an independent, private foundation that works for the positive development of the internet."[6]

SIDN (Netherlands) does not mention development of the Internet specifically, but refers to the development of products to support its mission of "connecting people and organisations to promote safe and convenient digital living."[7]

DENIC (Germany) "are actively involved in shaping the further evolution of the Internet by participating in international bodies" and "support the further evolution of the Internet by sponsoring dedicated projects and events."

DIFO (Denmark) notes that "it is our civic duty to operate and further develop the .dk domain, continuing to put a stamp of quality on even more first-rate digital experiences that bring people together and create new relations." It also states that it will "will ensure user-friendly services and contribute to global cooperation that promotes a well-functioning and secure internet."[8]

Focus on consumers and responsiveness to user needs

In most of the ccTLD principles, there are statements on the importance of connecting with and being responsive to users.

The Swedish Internet Foundation has a particularly unique characterization: "...We are responsible for the Swedish top-level domain .se and the operation of the top-level domain .nu, and our vision is that everyone in Sweden wants to, dares to and is able to use the internet."

For SIDN (Netherlands), "Our mission is connecting people and organisations to promote safe and convenient digital living. We seek to do that by keeping the .nl domain as stable and secure as possible, by using our expertise to promote internet security, and by developing new products and services that support our mission." Its experts are working "to make sure that you can have confidence in your digital world."

[6] https://internetstiftelsen.se/en/we-are-the-swedish-internet-foundation/
[7] https://www.sidn.nl/en/about-sidn/our-organisation
[8] https://www.difo.dk/en/strategy

SIDN's vision is that the Internet is "the medium for information exchange, social interaction, cooperation and commerce. It also supports the economic and democratic development of nations and the personal development of individuals."

In its Corporate Profile, JPRS (Japan) identifies the following as core concepts for services with a particular focus on users/customers: "Usability: providing accessible services which meet users' needs" and "Fee Performance: providing services at reasonable fees."

Recognizing the importance of the customer is central to DIFO and DK Hostmaster (Denmark) : "We play a major role in the digital lives of the Danes. This means we must earn their trust. We are therefore committed to strengthening and securing digital identity, to ensure that everyone knows who they are dealing with when they shop, meet and communicate online. We collaborate closely with our customers and the entire internet community; always advancing towards a better and safer internet."

DK Hostmaster states in its "About" page that they are "aware that we are entrusted with something vital to both our customers and their businesses." And that "Our aim is to provide stable and reliable operations as well as the highest level of security and service, aligned to the day-to-day realities of our customers – which perpetually pose new challenges. Consequently, we are constantly evolving and progressing with and for our customers, to help them focus on what they do best."

What are the overarching principles that guide ccTLD policies in specific areas?

Such areas include:

- Indigenous rights or multiculturalism
- E-commerce
- Security
- Competition
- Human rights
- Privacy
- Openness
- The rights or interests of registrants

Indigenous rights or multiculturalism

There are no specific mention of indigenous rights as principles.

SIDN (Netherlands) in its vision statement notes under the principles of “Open and accessible” that it wants “a single, global internet that is open and accessible to all and reflects the world's diversity of cultures, languages and scripts. ...” suggesting that the single global Internet will encourage diversity and multiculturalism/multilingualism.

E-commerce

There are very few specific references to e-commerce, although there is a considerable focus on consumers and users (see the section above on Focus on consumers and responsiveness to user needs.)

Security

(See the section above on Security)

Competition

No specific references at the principles level.

Human rights

There are few direct references to human rights or principles that would facilitate rights being realized although, as is typical in the DNS space, there are numerous references that can be associated with rights.

The Swedish Internet Foundation specifically mentions Human Rights in its Code of Conduct: "Human Rights: All activities should follow the guidelines of international conventions concerning basic human rights. Use of slave or child labour is completely unacceptable. The Swedish Internet Foundation also works to exclude the presence of controversial minerals in our business or supply chain."

DENIC (Germany) states that it advocates for "diversity of opinion and freedom of participation in the network of networks." It also strives "to preserve the Internet as a forum for many and a space for global exchange, as a platform for innovation, creativity and business ideas that works across traditional borders." Again no specific mention of human rights, but references to issues that are associated with rights more broadly.

It should be noted that human rights and openness are often associated in the broader context of Internet Governance and this can be found in the principles for the ccTLDs, as discussed further below.

Privacy

No specific references at the principles level.

Openness

The notion of openness is a recurring theme and central to the characterisation of the Internet as global, open and free. This is a theme that is found across ccTLD websites.

SIDN (Netherlands) in its vision statement notes under the principles of "Open and accessible" a number of human rights, including free expression: "We want a single, global internet that is open and accessible to all … An internet where freedom of expression, the right of publication and unrestricted access to information are the norm. So that you and all other internet users are entitled to feel secure."[9]

[9] https://www.sidn.nl/en/about-sidn/what-we-stand-for

DENIC (Germany) similarly associated openness with rights: “Are committed to a free Internet, which is open to everyone.”

In realizing its vision and mission, DIFO’s (Denmark) strategy incorporates and “Open, secure and accessible internet for all” among others.

It should be noted that while there are few references to human rights, the notions of an open and accessible are often seen as encompassing a set of freedoms that are typically associated with human rights, such as free expression.

The rights of registrants

None specifically although inferred from principles related to consumers.

Additional principles

Internet Governance related principles

As mentioned above, there are a number of references to Internet Governance and the Internet ecosystem in the principles articulated by the ccTLDs.

It is worth noting in full the importance of Internet governance themes and multistakeholderism for DENIC (Germany):

“Internet Governance: Part of DENIC’s key set of values. DENIC does not only view its core task – i. e. ensuring Internet users’ fast, secure and reliable access to webpages and services under Germany’s country code TLD .de - as a social mission. The Cooperative also actively promotes the multistakeholder model in the context of Internet Governance and has been constantly involved in a multitude of IG organisations for many years: Multistakeholderism is a pluralistic approach that unites different stakeholders - from representatives of governments and international organisations to the private sector, academia and civil society to the technical infrastructure operators of the Internet (like DENIC itself). All these stakeholders join together to develop rules, values and standards related to the Internet of the presence and the future on an equal footing. And all of this is achieved bottom up instead of top down.”[10]

Many of the same values were articulated by the technical community in its contribution to the 2013 NetMundial meeting in Sao Paulo, Brazil in April 2014. Both DENIC (Germany) and JPRS (Japan) were signatories to the “Internet Governance

[10] https://www.denic.de/en/whats-new/features/our-contribution-to-a-secure-internet-for-all/?tx_denic_notification%5Bnotification%5D=116&tx_denic_notification%5Baction%5D=acknolwedge&tx_denic_notification%5Bcontroller%5D=Notification&cHash=ad54484fb2bc3230ba6f8862d2f36d8e

Observations and Recommendations from Members of the Internet Technical Community“ statement (as was InternetNZ).[11]

Principles specifically related to corporate standards/employee behaviour

It is also worth mentioning, as noted above, the Swedish Internet's Foundation extensive code of conduct designed to assist in achieving its mission of promoting "stability in the Swedish internet infrastructure as well as promote the spread of knowledge about the internet and electronic communication." The code of conduct is based on the UN's Global Compact and applies to all employees. See the Annex for the Code in its entirety, or here.

[11] https://www.internetcollaboration.org/ig-recommendations-itcg/

Principles by ccTLD

In this section, we have listed the principles as stated by each ccTLD registry.

Sweden

The Swedish Internet Foundation vision:[12]

> "The Swedish Internet Foundation is an independent, private foundation that works for the positive development of the internet. We are responsible for the Swedish top-level domain .se and the operation of the top-level domain .nu, and our vision is that everyone in Sweden wants to, dares to and is able to use the internet."

This said, the purpose of the Swedish Internet Foundation and operating regulations can be found in the charter of foundation, including the associated statutes:

> "The Foundation's purpose is to promote positive stability in the internet infrastructure in Sweden and to promote research, training and education in data and telecommunication, with a specific focus on the internet. By so doing, the Foundation must assign priority areas that increase the efficiency of the infrastructure for electronic data communication, whereby the Foundation, inter alia, shall disseminate information concerning R&D efforts, initiate and implement R&D projects and implement high-quality inquiries. The Foundation must particularly promote the development of the handling of domain names under the top-level domain ".se" and other national domains pertaining to Sweden.
>
> Promoting positive stability in the internet infrastructure could, for example, entail handling the administration and registration of domain names, supporting the establishment, operation and build-out of internet centers in Sweden and supporting the operation of joint resources, such as directory systems and the distribution of exact time."

Importantly, the Swedish Internet Foundation follows a Code of Conduct based on the ten principles of the UN's Global Compact when implementing its mission. The Code supplements and summarizes the Foundation's different policies, employee handbook and governing. It embraces a number of issues: human rights; employee and working environment; anti-corruption; environmental responsibility; and, privacy and information. The code can be found here.

[12] https://internetstiftelsen.se/en/

Germany

DENIC's principles and mission:[13]

> ***"Responsibility for the Internet Community***
>
> We work in keeping with the principles of RFC1591, in which the requirements for the administration and operation of ccTLDs are defined:
>
> - We have a duty to serve the Internet community.
> - We are able to carry out the necessary responsibilities, and have the ability to do an equitable, just, honest and competent job.
> - Our legitimation is based on our being rooted in and recognised by the local Internet community.
>
> As the central registry for .de domains, we fulfil our tasks as a not-for-profit organisation, for the benefit of the entire Internet community. Our fundamental principles are impartiality, independence, technical expertise, responsibility and non-discrimination."

Further, DENIC's activities are guided by the fundamental principles laid down in its Statutes:

- Work on a not-for-profit basis
- Provide important services for the benefit of not only the German, but the global Internet community
- Are committed to a free Internet, which is open to everyone
- Are actively involved in shaping the further evolution of the Internet by participating in international bodies
- Act independently, responsibly and free from discrimination, in line with international standards for domain registries.

DENIC also places significant importance on its engagement in and support for the broader Internet Governance ecosystem and the principles that underpin it, as exemplified by its Internet Governance Radar.

[13] https://www.denic.de/en/about-denic/our-mission/

Netherlands

On SIDN's "What we stand for" page[14] the ccTLD manager outlines both its mission and vision, and embodies a set of principles:

> "**Our mission**: Connecting people and organisations in a secure digital world.
>
> **Our vision**:
>
> Vital medium
>
> The internet has become the medium for information exchange, social interaction, cooperation and commerce. It also supports the economic and democratic development of nations and the personal development of individuals.
>
> Quality and security
>
> In the years ahead, the internet will be used ever more intensively by ever more people. It will also become possible to do more things on the internet. Against that background, it's vital that people can be confident in the internet's quality, security and privacy.
>
> Independent experts
>
> We work to make sure that you can have confidence in your digital world. We deliver high-quality services linked to innovative, secure domains and digital identities. By doing that, we add to the social and economic value of the internet for the Netherlands and the wider world. We are experts in our field and we operate on a completely independent basis.
>
> Open and accessible
>
> We want a single, global internet that is open and accessible to all and reflects the world's diversity of cultures, languages and scripts. An internet where freedom of expression, the right of publication and unrestricted access to information are the norm. So that you and all other internet users are entitled to feel secure."

According to its Constitution, SIDN's objective is to:

[14] https://www.sidn.nl/en/about-sidn/what-we-stand-for

"provide added value for the Internet community by developing and maintaining (against reasonable charges) services and products connected with digital registration and/or network resolving, such as domain name systems (including a system for the .nl domain), and by undertaking any other activities directly or indirectly associated with or conducive to the said end, all in the broadest sense of the words."

Denmark

The Danish Internet Forum (DIFO) sets out the strategy for DK Hostmaster, the administrator of the ccTLD. The two organisations have a joint vision and mission:[15]

"**Vision**

DIFO and DK Hostmaster will be among the best domain name administrators in the world."

Mission

We will ensure user-friendly services and contribute to global cooperation that promotes a well-functioning and secure internet."

Strategy

In continuation of the above vision and mission, our three main strategic areas of focus are:

- Protection of a consumer-oriented focus
- Open, secure and accessible internet for all
- Full transparency in DIFO's decision-making processes, nationally and internationally.

DK Hostmaster has a further set of "principles" including:

"Our aim is to provide stable and reliable operations as well as the highest level of security and service, aligned to the day-to-day realities of our customers – which perpetually pose new challenges. Consequently, we are constantly evolving and progressing with and for our customers, to help them focus on what they do best.

[15] https://www.difo.dk/en/strategy

We are therefore committed to strengthening and securing digital identity, to ensure that everyone knows who they are dealing with when they shop, meet and communicate online.

We collaborate closely with our customers and the entire internet community; always advancing towards a better and safer internet.

It is our civic duty to operate and further develop the .dk domain, continuing to put a stamp of quality on even more first-rate digital experiences that bring people together and create new relations."[16]

Japan

JPRS' mission is as follows:

> "As a company dedicated to maintaining the Internet infrastructure of Japan, Japan Registry Services (JPRS) contributes to the development of the Internet and the building of a better future for everyone."[17]

Its corporate philosophy:

> "As a company dedicated to maintaining the network infrastructure, JPRS contributes to the development of the Internet and the building of a better future for everyone."[18]

The JPRS President's message includes a number of principles, particularly under the responsibilities section:

> "Supporting the Internet infrastructure for a better future
>
> The Internet has become an essential part of the groundwork for today's society. Especially, domain names are crucial to Internet access. Japan Registry Services Co., Ltd. (JPRS) supports the infrastructure of the Internet on a 24/7/365 basis through the management and administration of domain names and operation of the domain name system (DNS).

[16] https://www.dk-hostmaster.dk/en/dk-hostmaster
[17] https://jprs.co.jp/en/about/
[18] https://jprs.co.jp/en/about/corporate.html

Contributing to society through technology development and value creation for JP Domain Name

Keeping up with the latest technologies is indispensable for domain name management and DNS operations. As a company supporting the network infrastructure, JPRS must offer new services to society by applying the DNS related technologies it has developed and acquired through the operation of domain names. For that purpose, JPRS is actively researching and developing new technologies. JP domain names are accessible not only inside Japan, but also from all over the world. Therefore, in the interest of both the global community and the community in Japan, JPRS is developing, improving, and promoting its services to ensure that JP domain names are more user-friendly and have higher value.

Responsibilities as a company supporting the network infrastructure

As a company dedicated to supporting the network infrastructure, we strive to maximize reliability and respond to the expectations of the community. Moreover, we support the evolution of the Internet by coordinating closely with Internet-related organizations at home and abroad as well as the Government of Japan. JPRS will keep making every effort to contribute to society into the future."

South Africa

While both ZADNA (the manager) and ZACR (the registry) have "about" pages and mandates, etc. neither have a specific list of principles that guide their organizations. ZADNA's mandate is here. ZACR's "about page" highlights some of its achievements and various initiatives being undertaken with registrars here.

Privacy

How do the policies of the ccTLDs treat the privacy of registrant data (the private information of the registrant)?

Overview

The European Union's General Data Protection Regulation[19] is the most significant driver of change in data privacy as it impacts the domain name system. GDPR is shaping both general privacy provisions and access to registrant data within and beyond the European Union. For European ccTLD operators, there remain some slight but interesting variations in approaches to data privacy as noted below.

Netherlands

For .nl, the following limited information is published in the WHOIS: "the registrant's name (if the registrant is a business), the e-mail addresses of the administrative and technical contacts, details of the registrar, and technical data….". To access additional information, SIDN can share information with those who have legitimate interests in accessing the data (assuming they satisfy certain criteria) and with investigative or enforcement authorities, subject to a request to the ccTLD.

SIDN also provides a further privacy enhancing "opt-out" option[20] allowing for a registrant to "withhold their name (in circumstances where it would ordinarily be published) and the e-mail addresses of their administrative and technical contacts from the publicly accessible part of our database, and to replace the information in question with the contact details of their registrar."

The ability to "opt-out" is not a given: the request is more likely to be granted if, for example, "You have a material interest in anonymity; the issue behind your request has been reported to the police; [and/or] you've already taken steps to protect your privacy elsewhere." The Opt-out page notes that "Your request won't be approved if you want to opt out simply to avoid spam or because someone has a grudge against you. Those are everyday problems that don't outweigh the reasons for publication."

Germany

DENIC's approach to privacy is also driven by GDPR. Following a review of its data processing procedures in 2018, DENIC announced changes with regard to the collection and publication of registration data:

[19] https://gdpr-info.eu/
[20]https://www.sidn.nl/en/nl-domain-name/opt-out-requests

https://www.denic.de/en/whats-new/press-releases/article/extensive-innovations-planned-for-denic-whois-domain-query-proactive-approach-for-data-economy-and/

These include a set of fields limited to technical data, information for establishing contact for inquiries – one for general requests and another for abuse – and information about the domain holder. The latter is restricted to the domain holder themselves, and to parties that may have a legitimate interest if there has been a name or trademark violation or if the requesting party has possible unlawful or improper use of the domain (this form), etc., through a set of forms provided by the ccTLD.

Sweden

As with DENIC, the Swedish Internet Foundation does not provide contact ID for natural or sole proprietorship registrants in WHOIS look-ups. It does provide date created and date of expiration fields, as well as a form to contact the registrant. If the registrant identifies themselves as a legal entity (corporation) the contact data is made available in the WHOIS look-up.[21] There appears to be no particular opt out/opt in provisions.

Denmark

.DK Hostmaster takes a very different approach. Section 18(1) of the Danish Domain Names Act ensures transparency of Danish domain names by making details such as a user's name, address and telephone number publicly available in the WHOIS, whether the registrant is an organization or an individual. This legal basis is deemed sufficient for the continued publication of the data despite what may appear to be a conflict with GDPR.[22] This said, it is acknowledged that should the continuation of publishing data that contradicts GDPR be "deemed unlawful, the publication of proxy data will cease and the registrant agreement will be changed accordingly."[23]

While transparency is paramount, there is a provision in the Danish Domain Names Act that can be used to secure name and address anonymity in the WHOIS. This provision for anonymous registrants is based upon the ability to seek name and address protection under the Danish Civil Registration System. DK Hostmaster compares its data with the Danish National Register of Persons so that users with name and address protection in the register are also protected at DK Hostmaster, and therefore in the WHOIS.[24] Similarly, if a registrant's telephone number is

[21] https://internetstiftelsen.se/app/uploads/2019/02/integritetspolicy-se-eng.pdf
[22] https://www.dk-hostmaster.dk/en/gdpr
[23] https://www.dk-hostmaster.dk/en/node/473
[24] https://www.dk-hostmaster.dk/en/anonymity

unlisted, it will also be hidden. Registrants outside of Denmark can also be listed as anonymous if they have the equivalent of the Danish name and address protection in their country of residence (this requires that appropriate documentation showing the same levels of protection in the registrant's country is made available).

Japan

Unclear if there are enhanced privacy protections and whether they are optional. The JPRS privacy policy documents can be found here, in Japanese.

[While ICANN's Temporary Specification for gTLD Registration Data does not apply to ccTLDs, JPRS has an interesting guide for WHOIS/JPRS RDAP compliance: https://jprs.jp/registrar/info/gdpr/gdpr-index-en.html#3-gtldwhois]

South Africa

The privacy policy for ZADNA can be found here: https://www.registry.net.za/downloads/u/ZACR_Privacy_Policy.pdf

There appear to be no explicit opt out/opt in approaches to enhanced privacy provisions.

Indigenous rights

How do the policies of the cc TLDs reflect the rights of indigenous peoples?

For example:

- Are there policies that consider the offensive use of indigenous language in domain names?
- Are there any other exceptions to the first come first served approach?

Summary

None of the ccTLDs reviewed had specific policies that reflect the rights of indigenous or minority peoples. Nor are there any policies that consider offensive use of indigenous language in domain names – in some there are general provisions for domains that "could cause offense". A number of the ccTLDs have incorporated additional characters to enable the fullest use of the character sets associated with the official and minority languages. All the ccTLDs have first come first served approaches to domain registration. There are largely no exceptions.

Sweden

It does not appear that The Swedish Internet Foundation's (SIF) policies refer to the rights of indigenous or minority peoples.

However, as of 2007, Swedish minority languages were accounted for as .se domain could contain "all the letters required to write in Swedish and the Swedish official minority languages (Finnish, Meänkieli (Tornedal Finnish), Sami, Romani and Yiddish)..." including "... the letters required for writing in Finnish, Norwegian, Danish and Islandic. This means that it is possible to use letters such as å, ä, ö, ü and é in a .se domain."[25] A useful overview of IDNs and IDN support for .se can be found here and the list of available characters is available here.

A recent report from the Swedish government to the Council of Europe on minority peoples and languages in Sweden (for background: no Internet or DNS references) can be found here.

There appear to be no exceptions to the first come first served principle. Section 3.1.2 of the Terms and Conditions of Registration states that "For new registration of Domain Names, a 'first come, first served' principle, which means Domain Names are

[25] https://internetstiftelsen.se/en/how-to-register-a-domain-name/terms-and-conditions-for-se-and-nu-domains/

allocated in the order in which the applications are entered in The Swedish Internet Foundation's register."[26] This is reinforced by the following: "There are no possibilities of priority registration or reservation of domain names."[27]

The registration T&Cs under 4.2 also note that "The Domain Holder is obliged at all times to ensure that the Domain Name selected does not constitute an infringement of the rights of another party, nor in any other way constitute a violation of applicable statutes or public order, and is not intended to cause offence." Whether or not the latter refers to offense in the sense of the use of offending words in the official languages is unclear.

As noted elsewhere, certain names are reserved/blocked and can be found here.

Germany

As with SIF, DENIC does not refer to indigenous or minority peoples (note: there are eight recognized minority languages in Germany).

With regard to encouraging linguistic diversity, DENIC lists the 93 additional characters (internationalised domain names or IDNs) that are allowed in the .de domain (including the umlaut and the eszett) and provides useful pages on IDNs and comprehensive FAQs. DENIC also provides links to an IDN converter tool and to IDN capable software.

For .de domain registration, DENIC handles these on a strictly first come first served basis. The Domain Guidelines state that "DENIC will register the domain if it has not already been registered for someone else ("first come, first served") and provided that it is not in the Redemption Grace Period. It may, however, reject the application if it is obvious that the registration would be illegal."[28]

Netherlands

As with SIF and DENIC, SIDN does not explicitly refer to indigenous or minority peoples (although The Netherlands has minority languages).

With regard to **first come first served**, SIDN in its General Terms and Conditions for .nl Registrants states that: "1.3 We use automated systems to process applications in the order that we receive them. On receipt of an application, we check first whether the .nl domain name is available for registration, and then whether the application is

[26] https://internetstiftelsen.se/app/uploads/2019/02/registreringsvillkor-se-eng.pdf
[27] https://internetstiftelsen.se/docs/Terms-and-conditions-and-rules-for-registering-domain-names-with-.se_.pdf
[28] https://www.denic.de/en/domains/de-domains/domain-guidelines/

complete and correct. We register a .nl domain name to the first applicant whose application for the name passes both the checks."

In the following paragraph, it states "If there are technical reasons for not registering one or more .nl domain names, we can refuse the application or applications." And "We can also temporarily exclude a .nl domain name from registration, if the Complaints and Appeals Board has ruled that the name in question is inconsistent with public order or decency."[29]

Denmark

Neither DIFO nor DKHostmaster mention indigenous or minority peoples.

All characters In Danish are available to use when registering a domain name, including æ, ø and å. There appears to be no (other) mention of IDNs.

With regard to the first come first served principles, DK Hostmaster states that "All .dk domain names belong to the sovereign state of Denmark and are managed by DIFO / DK Hostmaster according to the first-come-first-served principle".[30]

Japan

Neither JPNIC nor JPRS mention indigenous or minority peoples.

JPRS launched its first come first served[31] registration application period for .jp domain names in 2001.

JPRS is also promoting IDNs through its registration service for Japanese JP Domain Names.[32]

South Africa

Neither ZADNA nor ZACR mention indigenous nor minority peoples (note: South Africa has 35 indigenous languages, 10 of which are official.)

However, in its mandate "ZADNA may, with the approval of the Minister of Communications, make regulations regarding: The circumstances and manner in which registrations may be assigned, registered, renewed, refused, or revoked by the

[29] https://www.sidn.nl/downloads/d_7zdiiDQvOGbSo1FGCcqw/d4c8288846f98ba422834c996994a04a/General_Terms_and_Conditions_for_nl_Registrants.pdf

[30] https://www.dk-hostmaster.dk/en/welcome-dk-hostmaster

[31] https://jprs.co.jp/en/regist.html

[32] https://jprs.co.jp/en/jdn.html

registries with due regard to the express recognition of the right of groups and members of groups within the Republic to identify with, use or communicate cultural, linguistic, geographical, indigenous or any other expressions of heritage including any visual or audible elements or attributes thereof ...."[33] This said there appear to be no references to ZADNA having made regulations with regard to indigenous matters.

In the 2015 ZA Second Level Domain General Policy, the first come first served principle is addressed, as well as exceptions and obligations:

> 1.4.1. Under normal circumstances, a Domain Name is registered on a first-come, first-served basis, unless otherwise stated in a Charter. An SLD launch plan may include phases that allow certain classes of applications to be made on bases other than first-come, first-served, such as sunrise and land rush phases.
>
> 1.4.2. In registering and renewing a .ZA Domain Name, a Registrant is deemed thereby to be warranting the Registrant's compliance with any applicable eligibility and usage criteria.
>
> 1.4.3. Neither ZADNA nor Registry has any obligation to determine whether or not Registrants of .ZA Domain Names comply with any applicable eligibility or usage requirements. By registering a Domain Name in a Restricted SLD, the Registrant warrants that s/he or it is eligible to register and use the Domain Name. Administrators of Restricted SLDs may require Registrants to submit proof of their eligibility to register in the Restricted SLD.[34]

It is interesting to note that while there are no policies yet for indigenous peoples, ZADNA led the efforts to secure the South African city TLDs .Capetown, .Durban and .Joburg in 2014.[35]

[33] https://www.zadna.org.za/content/page/our-mandate/
[34] https://www.zadna.org.za/uploads/files/ZA_SLD_General_Policy_final_1_April_2015.pdf
[35] https://www.zadna.org.za/content/page/za-cities-tlds1/

Prohibited word lists

Which ccTLDs have prohibited word lists and how do they operate?

Summary

Of the 6 ccTLDs reviewed, it appears that not one has a list of prohibited words.

It should be noted however that in some cases there are blocked or reserved lists of domain names, but these are typically to prevent confusion with citizen identification numbers, IDNs, international organisations, government or geographic designations, etc. , as well as limitations on characters that can be used within a domain name.

The above have been touched upon below.

Sweden

There is no prohibited words list.

The Swedish Internet Foundation lists the following as “blocked”:

- Domain names that consist of number combinations in the format xxxxxx-xxxx and xxxxxxxx-xxxx since they are or may be confused with personal identity numbers.
- Domain names that contains of two letters followed by two hyphens as they could be confused with IDNs, and
- Designations related to international humanitarian law and the law and certain other official designations.

The full list of blocked names can be found here. In addition, domain names cannot conflict with the law or infringe on the rights of others, such as a trademarks, etc.

Accepted characters are as follows:

“A .se or .nu domain may contain at least one and at most 63 characters ... the letters a-z, numbers 0-9, hyphens, and all the letters required to write in Swedish and the Swedish official minority languages **(Finnish, Meänkieli (Tornedal Finnish), Sami, Romani and Yiddish)**. It may also contain the letters required for writing in Finnish, Norwegian, Danish and Islandic. This means that it is possible to use letters such as å, ä, ö, ü and é in a .se domain.” The full list of characters can be found here.

It is worth noting that that the registrant is obliged to ensure that the “domain name selected does not constitute an infringement of the rights of another party, nor in any

other way constitute a violation of applicable statutes or public order, and is not intended to cause offence." If the domain name is found to "violate Swedish legislation or statutes, The Swedish Internet Foundation has the right to immediately deactivate or deregister the domain name."[36]

Germany

There does not appear to be a prohibited words list.

As with.se, DENIC provides the following on the characters and parameters for acceptable domain names:

"A valid domain must be comprised solely of the digits 0-9, the 26 letters of the Latin alphabet, the hyphens and the other letters listed in the Annex of the DENIC Domain Guidelines. Hyphens are not permitted in first or last place, nor is it possible for both the third and fourth places to be hyphens at the same time (such as xn--.de). No distinction is made between capital and small letters (upper and lower case). The minimum length of a .de domain is one character and the maximum length is 63 characters (cf. RFC1035). If the domain includes letters from the Annex, the maximum length is determined by its ACE version in accordance with RFC3490."[37]

Annex of letters: https://www.denic.de/en/domains/de-domains/domain-guidelines/

Netherlands

There does not appear to be a prohibited words list.

The following was worth quoting in full: "In the Benelux, domain names are almost never refused on the grounds of public order or decency. Elsewhere, it depends on the culture. It's some years since a .nl domain name was last refused on public order or decency grounds. Nevertheless, if you think a name is unacceptable, you can report it to the Complaints and Appeals Board (C&AB)."[38]

Denmark

There does not appear to be a prohibited word list.

[36] https://internetstiftelsen.se/app/uploads/2019/02/registreringsvillkor-se-eng.pdf
[37] https://www.denic.de/en/domains/de-domains/domain-guidelines/
[38] https://www.sidn.nl/en/internet-security/protecting-yourself-against-internet-abuse-in-the-netherlands-and-in-gtlds

The approved character list for domain names can be found here. This is not dissimilar to the Swedish and German lists.

Japan

There does not appear to be a prohibited words list.

There is a document dating from 2001 that lists reserved domain names (in Japanese): http://www.nic.ad.jp/dotjp/doc/dotjp-reserved.html

For an English listing from the same date see pages 9, 10 and 11 of this pdf.

South Africa

There does not appear to be a prohibited words list.

Human Rights

How do the policies of ccTLDs consider and give effect to human rights?

- Is the focus mainly on freedom of expression or are other human rights (such as freedom from discrimination, right to life, liberty and security of the person) considered? Either way, how are the rights reflected or addressed in the policies?
- Is there specific provision to enable vulnerable people (such as those with disabilities, aged community, minorities, LGBT community, and the digitally excluded) to access registry services?

Overview

As noted in the general overview of principles, there are few specific mentions of human rights at a mission/vision or principles level. This said there are numerous references to freedoms and other key principles associated with human rights and their realisation. Central to these are the importance of development and governance to ccTLDs, and the notion of being able to access a global Internet. The themes of openness and accessibility are often articulated together.

While there may not be any specific policies that "give effect to human rights", the broader question of Internet governance and the policies – whether technical or regulatory – that ccTLDs and other actors in the Internet ecosystem adopt or abide by directly or indirectly do have an impact on how users connect, how they share information and how they express themselves, effectively shaping their human rights in the context of the Internet more broadly.

There are few references to vulnerable people in the ccTLDs reviewed.

Sweden

Rights come to the fore for The Swedish Internet Foundation (SIF) in terms of the tension between free expression and illegal content: "The Swedish Internet Foundation is favourable to an open internet that protects freedom of speech. At the same time, it is important that there are legal and effective tools for working against criminal activities and illegal content online." SIF's position is made clear: "It is not the role of The Swedish Internet Foundation, but the judiciary, to determine whether

certain content is legal or illegal. In this way, important aspects such as freedom of expression and rule of law are taken into account."[39]

The Swedish Internet Foundation specifically mentions human rights in its Code of Conduct: "Human Rights: All activities should follow the guidelines of international conventions concerning basic human rights. Use of slave or child labour is completely unacceptable. The Swedish Internet Foundation also works to exclude the presence of controversial minerals in our business or supply chain."[40]

Germany

DENIC states that it advocates for "diversity of opinion and freedom of participation in the network of networks."[41] It also strives "to preserve the Internet as a forum for many and a space for global exchange, as a platform for innovation, creativity and business ideas that works across traditional borders." Again no specific mention of human rights, but references to issues that are associated with rights more broadly.

It should be noted that human rights and openness are often associated in the broader context of Internet Governance and this is reflected in a number of places on the DENIC website. In particular:

Therefore, hardly any issue exists in the political, economic or sociocultural sphere today that is not somehow related to or influenced by the Internet: On the one hand, technical rules and government regulations on cyber security have an impact on business models and determine to what extent individuals may exercise specific human rights, such as the freedom of expression or the right to privacy. On the other hand, technical rules and government regulations designed to grant privacy have an effect on and influence the digital economy and security on the Internet.[42]

The Netherlands

SIDN's vision is explicit in the importance that the ccTLD places on openness and accessibility:

We want a single, global internet that is open and accessible to all and reflects the world's diversity of cultures, languages and scripts. An internet where freedom of expression, the right of publication and unrestricted access to information are the norm. So that you and all other internet users are entitled to feel secure.[43]

[39] https://internetstiftelsen.se/en/who-takes-responsibility-for-content-online/
[40] https://internetstiftelsen.se/en/we-are-the-swedish-internet-foundation/code-of-conduct/
[41] https://www.denic.de/en/whats-new/features/our-contribution-to-a-secure-internet-for-all/
[42] https://www.denic.de/en/whats-new/features/internet-governance-matters-to-everyone
[43] https://www.sidn.nl/en/about-sidn/what-we-stand-for

A number of the SIDN Fund projects address accessibility issues, including the Continuous Accessibility Checker, a tool for checking during the testing phase how accessible new software is for people with impaired vision. The range of projects receiving recent funding can be found here.

There is an Accessibility Foundation in The Netherlands that works to improve the accessibility of the Internet and other digital media for all people, including the elderly and people with disabilities. (It is unclear whether or not SIDN works with this Foundation).

Denmark

DIFO's strategy in delivering its vision and mission includes an "open, secure and accessible internet for all" as one of its three main strategic areas of focus.[44] As mentioned above, however, these tend to be general characteristics more associated with the broader themes of Internet governance than human rights specifically.

The Danish Act on Internet Domains provides the basis for the administration of .dk domains handled by DIFO and DK Hostmaster. The Act "also guarantees the user a number of rights as well as the option to bring a dispute about domain names before a complaints board." [Note: the Act is in Danish.] However, it is unclear to what degree these "rights" in the Act are rights in the sense of human rights.

Japan

[Unable to find anything of relevance]

South Africa

As noted elsewhere, ZADNA may, with the approval of the Minister of Communications, make regulations regarding:

The circumstances and manner in which registrations may be assigned, registered, renewed, refused, or revoked by the registries with due regard to the express recognition of the right of groups and members of groups within the Republic to identify with, use or communicate cultural, linguistic, geographical, indigenous or any other expressions of heritage including any visual or audible elements or attributes thereof....[45]

[44] https://www.difo.dk/en/strategy
[45] https://www.zadna.org.za/content/page/our-mandate/

Although the enumerated areas could be directly or indirectly associated with human rights it is unclear if any such regulations have been developed and enacted. Most of the rights related activity at ZADNA has to do with the protection of intellectual property rights.

ZACR has a programme that "target schools in under-resourced communities where education, training and digital literacy development are critical for the sustainability of the Information and Communications Technology (ICT) environment. We aim to install world-class computer environments in our schools." While not specifically addressing human rights, the intent and purpose of the programme is to enable school children to realize their rights.

ZACR also manages the domain space for org.za, the Charter for which notes that "potential registrants include, but are not limited to, charities, non-governmental organisations (NGOs), non-profit companies (NPCs), trade, industry and civil society associations, trade unions, political parties and religious organisations … " typically those that are aware of or actively promote human rights and rights online."[46]

There were no specific references to vulnerable people beyond those noted above in the ZADNA mandate.

[46] https://www.zadna.org.za/uploads/files/Final_ORG_ZA_Charter_31July2014.pdf

Growth and innovation

Are there any policies or programs that explicitly or implicitly support growth, innovation and consumer "power"?

Summary

Most of the reviewed ccTLDs put in place policies and/or programs that address specific domain name issues, such as security, rather than broader consumer and business related issues. These range from typical measures to address DNS abuse such as phishing and malware, to others designed to reduce the likelihood of inadvertently losing a domain name. While there are policies and programs that increase consumer security, there are none that directly increase consumer "power" in the domain name market. Under the broader umbrella of efforts to address innovation and implicitly growth, ccTLDs (some not all) provide a range of programs[47], from funding innovation, to administering or providing registry services for other domains, notably cities.

Sweden

The Swedish Internet Foundation (SIF) is clear in its purpose as "an independent, business-driven and public-benefit organization" that works "**for an internet that contributes positively to people and society**". There is recognition of the need to constantly improve services and contribute to Internet development: "**The revenue from our business finances a number of initiatives in order to enable people to use the internet in the best way, and to stimulate the sharing of knowledge and innovation with a focus on the internet.**" SIF's goal is to invest at least 25 percent of turnover in internet-related projects.[48]

In addition to more typical security related offerings, SIF has a number of projects that empower domain name holders and Internet users in a variety of ways, from publishing a list of domain names that may become available, to providing a broadband speed test. SIF funds an open work space called Goto 10 for internet related knowledge exchange and innovation, including a co-working space to promote internet related projects at an early stage; and, organizes the Swedish Internet Days conference.

The Foundation has also brought Internet service providers (ISPs), technicians and other stakeholders together as a part of the Project Internet Access to develop a measurement tool to assess when the Swedish Government's commitment to being a

[47] The programs mentioned provide a sense of the scope of programs offered by ccTLDs but are non-exhaustive.
[48] https://internetstiftelsen.se/en/we-are-the-swedish-internet-foundation/

"world leader in harnessing the opportunities of digital transformation" has been achieved.

Germany

DENIC works "as a not-for-profit organisation, **for the benefit of the entire Internet community**".[49] It is run as a cooperative: "the basic cooperative principles of self-help, self-responsibility and self-governance convinced the 37 founding members of the DENIC eG in 1996 to choose the organisational form of a cooperative. From the very beginning, they considered the management of the German namespace on the Internet and the provision of the necessary infrastructure a task to be tackled jointly." DENIC has a membership of over 300 Internet companies, a quarter of which are based outside Germany.[50]

DENIC is largely focussed on enhancing the security of domain names and registrants. Its offerings range from DENIC ID that enhances the user's security and digital identity when using log-ins, to DENICdirect which allows users the option of registering their domain names directly with DENIC without the usual suite of Internet services such as email, etc., to TRANSIT designed to protect the domain holder from unintended loss of a domain.

DENIC also sponsors or hosts a range of events, including EuroDIG and the Open ID Foundation, among others.

Where DENIC differs considerably from other ccTLDs is its focus on Internet Governance. While its Internet Governance Radar does not explicitly or implicitly empower businesses or consumers, it provides an incredibly useful tool for those interested to better understand the complex mix of the players, principles and policies.

Netherlands

Much like SIF, SIDN combines more traditional security enhancing offerings with funding other programs of broader but related impact. SIDN's focus on not just on security, but also quality: "In the years ahead, the internet will be used ever more intensively by ever more people. It will also become possible to do more things on the internet. Against that background, **it's vital that people can be confident in the internet's quality, security and privacy**.[51] SIDN works to "**deliver high-quality services linked to innovative, secure domains and digital identities. By doing that, we add to**

[49] https://www.denic.de/en/about-denic/our-mission/
[50] https://www.denic.de/en/whats-new/features/denic-cooperative-2018/
[51] https://www.sidn.nl/en/about-sidn/what-we-stand-for

the social and economic value of the internet for the Netherlands and the wider world."

SIDN's focus on secure domains and digital identities is exemplified by its acquisition in 2017 of Connectis, an identity infrastructure provider that connects organizations, sectors and nation: "the secure log-in solutions and reusable digital identities that Connectis provides are perfectly aligned with our mission."

The SIDN Fund is focussed on projects that make the internet stronger or promote the use the internet in innovative ways. Established in May 2014, with 5 million euros of start-up capital, the Fund is seen by SIDN as a way to "contribute to prosperity and welfare in the Netherlands". The range of funded projects can be found here. A good example of a project that encompasses both security and innovation supported by the Fund is Publicroam, a free, automatic and secure Wi-Fi service.

SIDN also supports a number of organisations that "promote digital skills, counter the internet's negative side-effects or contribute to internet-related innovation."

Finally, SIDN is also the registry for the geoTLD .amsterdam, providing more opportunities for using the domain name system to spur growth and creativity in and around the city.

Denmark

DK Hostmaster – a not-for-profit organisation – focuses on customers from a security and trust perspective: "Our aim is to provide stable and reliable operations as well as the highest level of security and service, **aligned to the day-to-day realities of our customers** – which perpetually pose new challenges and possibilities".[52] As noted elsewhere, DK Hostmaster promotes DNSSEC, DMARC and its VID or Very important Domain service to protect domain names from security breaches and human error. DK Hostmaster provides guidance on how to identify and report fake online shops, and offers courses on a variety of security and other topics.

Japan

In its corporate brochure, JPRS states that its core concepts for services are guided by, among others, the following: **usability - providing accessible services which meet user needs; and, fee performance - providing services at reasonable fees.**[53] It goes on to state that "JPRS is developing, improving, and promoting its services to ensure that JP domain names are more user-friendly and have higher value."

[52] https://www.dk-hostmaster.dk/en/dk-hostmaster
[53] https://jprs.co.jp/en/about/jprs-profile_en.pdf

As noted elsewhere, in addition to running .jp, JPRS is also running the TLD .jprs, the primary purpose of which is Internet research and development in an environment that will spur innovation.[54]

JPRS has also created an educational guide for younger persons on how the Internet works.

South Africa

ZADNA's mandate comes from the South African Electronic Communications and Transactions Act in which ZADNA "must enhance public awareness on the **economic and commercial benefits of domain name registration**." And in terms of the business environment for domain names "... may make regulations regarding - Processes and procedures to avoid **unfair and anti-competitive practices**, including bias to, or preferential treatment of actual or prospective registrants, registries or registrars, protocols or products."[55]

ZADNA has partnered on a project that specifically addresses business growth. In an effort to enhance the business opportunities to new companies the Companies and Intellectual Property Commission (CIPC), in partnership with ZADNA and ZACR, now offers domain name registration for any registered company, close corporation or co-operative, allowing them to register their own domain names before, during or after the company registration process.[56] ZADNA has also launched a Registrar Reseller Training Programme, the primary objective of which is to promote and create awareness of .ZA domain name and to grow the namespace, particularly by removing barriers to participation by SMMEs in townships and rural areas.[57]

And, through its cities TLDs and the SLDs org.za, co.za, gov.za and net.za, ZADNA and ZACR have provided for a diversity of South Africa focussed domains that should provide ample opportunity for consumer and business innovation and creativity in the domain industry in South Africa.

[54] https://jprs.co.jp/en/notice/whatisdotjprs-e.pdf
[55] https://www.zadna.org.za/content/page/our-mandate/
[56] https://www.zadna.org.za/projects/cipc-domain-registration/
[57] https://www.zadna.org.za/projects/za-registrar-reseller-development/

Local presence requirements

Do ccTLDs have geographic or country-based requirements for someone to acquire a domain name?

Summary

The six ccTLDs vary considerably in their country-based requirements for acquiring a domain name, from no restrictions whatsoever to local presence and domain based restrictions. In many cases the additional "local presence" requirements for legal purposes can and are provided through registry services.

Sweden

Registration requirements for .se domain names are largely the same for registrants inside and outside Sweden. According to terms and conditions of registration for the top-level domain .se from September 30 2019, "any natural person or legal entity with a personal identification number or corporate identity number, or that can be identified via a registration designation in a register maintained by a governmental authority, or by an organization exercising state authority, may apply for registration of a Domain Name under the top-level domain .se."[58] More specifically, for individuals or companies located in Sweden a valid Swedish personal ID or organizational number is required. Outside of Sweden any other ID number (e.g. Passport, driver's license, tax number) is accepted. Companies in the European Union must provide their VAT ID.[59]

Japan

For .jp registrations there are two categories. For general use, second level .jp domain names require a permanent postal address in Japan. Businesses applying for a 3rd level domain under co.jp need to be a corporation registered under the laws of Japan. Non-Japanese corporations registered in Japan as "Gaikoku Kaisha (Foreign Company)" may also apply for a co.jp domain name.[60]

[58] https://internetstiftelsen.se/app/uploads/2019/02/registreringsvillkor-se-eng.pdf
[59] https://iwantmyname.com/domains/se-swedish-domain-name-registration-for-sweden
[60] https://jprs.co.jp/en/regist.html#q1

Germany

For .de registrants not located in Germany there are additional requirements. DENIC requires that the non-domiciled registrant secure an authorised representative (or administrative contact or trustee – which some registrars can provide) in Germany to receive official or court documents for the registrant. Information to be provided for the representative or trustee should include their name and their full postal address.[61]

Netherlands

The Netherlands allows for the registration of domain names from around the world no matter the domiciliation of the registrant. This said, all .nl registrants whose addresses are outside the Netherlands require a "local agent" service (often provided by the registry) or local address - the SIDN address as a 'domicile address' is also available. This is so that there is a local Dutch address to which a bailiff or other can formally deliver official documents (e.g. a summons) to the registrant. SIDN may attach additional requirements on registrations that come from outside the European Union.

Denmark

There are no limitations as to registrations. However for Danish based registrants the registration data submitted and particularly the civil or business registration numbers must correlate with the same in the national CPR and CVR databases, respectively. The full procedure for local registrants can be found here. For registrants outside Denmark, DK Hostmasters performs a "risk assessment of the contact information provided in a domain name application" that may include requesting additional documentation to verify the address and identity of the registrant. The full procedure for non-resident registrations can be found here.

South Africa

There is no overall policy prohibiting non-South Africans from registering .za names, but most .za second level domains, especially the moderated ones (those subject to eligibility requirements), limit registrations to South Africans. However, the unmoderated (first come first served) - co.za and web.za -normally accept domain name registrations from both South Africans and non-South Africans.[62] Where a non-South African registers a .za domain name, there is usually a requirement that

[61] https://www.denic.de/en/domains/de-domains/domain-terms-and-conditions/

[62] https://www.zadna.org.za/content/page/domain-information/

the domain name holder consents to the application of South African law and jurisdiction of South African courts over any dispute involving the name.[63]

Website content regulation

Do the policies of the ccTLDs make any provision for regulating website content?

- If so, what content and in what circumstances?
- For example: To regulate fake online stores? To work with government agencies and other parties (trusted notifiers) to remove website content that is illegal?

Overview

Typically the ccTLDs in question provide information and other resources for those who believe that domains or websites may be used for abuse or purveying of illegal content, etc. At the same time, a number of ccTLDs are clear that their responsibilities do not extend to "regulating" website content nor to the purposes to which the domains are put (unless they breach particular terms and conditions), or the content they are associated with. It is not clear the degree to which the ccTLDs "work with" the authorities or merely refer illegal content to them.

Germany

Under the page on the DENIC website entitled Illegal Content - The Grey Area on the Internet[64] it states that "DENIC has nothing to do with either the contents or technicalities of websites accessible under .de domains. DENIC cannot determine the contents of websites nor can it exert any influence; it doesn't even have them saved on its own servers. All DENIC does is to provide the link between the domain and the website by registering the domain on its name servers."

This position is supported by a number of court cases., not least of which is the 'kurt-biedenkopf.de' finding by the Dresden courts that "DENIC was not subject to any sort of general obligation to check domains either prior or subsequent to their registration as to whether they might be the source of rights infringements." At the same time a court case in Germany also found that registrars could be held liable if they do not act swiftly enough to take down illegal websites.

[63] https://www.zadna.org.za/faq/registration/can-only-south-african-citizens-register-za/
[64] https://www.denic.de/en/know-how/illegal-content/

DENIC provides a contact list of organisations that have responsibilities for a range of types of illegal or harmful content, from harms to young people, spam mail, infringements of copyright, etc. DENIC is a founding member of The German Association for Voluntary Self-Regulation of Digital Media service providers (FSM e.V.) - a non-profit association responsible for protection of minors on the Internet.[65]

DENIC also has a page dedicated to fake online stores and lists relevant contact points for consumers as well as measures that can be taken by consumers to safeguard their transactions online. At the same time the ccTLD makes it very clear that it "can only assist affected parties who wish to claim their consumer or trademark rights against a fraudulent online shop" and not more broadly.

Under the DENIC Domains Terms and Conditions, the contract with the registrant can be terminated for a number of reasons including if "the registration of the domain for the Domain Holder manifestly infringes the rights of others or is otherwise illegal, regardless of the specific use made of it."[66]

Netherlands

Much like DENIC, SIDN provides numerous contact points and links to mechanisms that can address abuse. And much like DENIC it suggests that its role is minimal and provides avenues[67] through which action could be taken, from suggesting calling the police to contacting https://noticeandtakedowncode.nl/ to start a process among intermediaries to deal with reports of illegal content.[68] SIDN provides a list of parties to which the concerned party could complain, as follows: "Start with whoever put the content on the internet, e.g. the person that uploaded the video or posted the comments. If they won't take the material down, you can ask the next party up the chain. The chain is as follows: the content provider (uploader, writer); the website administrator; the registrant of the domain name; the registrar (hosting service provider); us, SIDN." If no party will take down the website or content, SIDN provides a takedown form for requesting that the ccTLD take action. SIDN does note however that "we can't take the content off the internet. We can break the link between the domain name and the website's IP address, making it hard for people to reach the content."[69] There is also a similar process via the Complaints & Appeals Board (C&AB)

[65] https://www.fsm.de/en
[66] https://www.denic.de/en/domains/de-domains/domain-terms-and-conditions/
[67] https://www.sidn.nl/en/internet-security/protecting-yourself-against-internet-abuse-in-the-netherlands-and-in-gtlds
[68] https://noticeandtakedowncode.nl/wp-content/uploads/2018/12/NTD_Gedragscode_English.pdf
[69] https://www.sidn.nl/en/nl-domain-name/complaining-about-the-content-of-a-website

[70] if there are concerns that a domain name is unethical or irresponsible.[71] An article on the pros and cons of take-down explores SIDN's approach in more detail.

In response to a recent consultation on the proposed amendment of the Dutch Consumer Protection (Enforcement) Act to ensure coherency with the European Union's Consumer Protection Cooperation Regulation, SIDN submitted a comment on domain name blocking and take-downs that acknowledges the need for such actions, but only as a last resort.

SIDN's tools and process for fake online store takedown is covered here. And, in 2020, SIDN published a paper on its successes in "Counterfighting Counterfeit: detecting and taking down fraudulent webshops at a ccTLD".[72]

Denmark

Much like DENIC and SIDN, DK Hostmaster suggests various avenues for addressing illegal content depending on the type of content in question.[73] Fraud and financial crime should be addressed to the police, unauthorized use of personal data to the Danish Data Inspectorate, and requests for takedowns referred to the Danish Courts.

However, DK Hostmaster has additional tools for addressing specific types of abuse/illegal content. The ccTLD can address typosquatting directly through its terms and conditions, for example. For issues of security and the public interest it takes a more engaged approach.[74] For DK Hostmaster to be able "to suspend a .dk domain name, two conditions must be met: 1) the Domain Name is used in connection with manifestly illegal acts or omissions that infringe substantial considerations of security or public interest, and 2) the circumstances call for not awaiting a decision from the Complaints Board for Domain Names[75] or the courts." Both conditions must be met before a domain name can be suspended. The provisions related to this can be found under section 9 of the terms and conditions for the right of use to a .dk domain name here.

DK Hostmaster also highlights the issue of fake online stores with guidance on how to determine the legitimacy of the site before purchasing goods online, including a comprehensive checklist of things to look for and the contact points for complaints, etc.

---

[70] https://www.cvkb.nl/en/
[71] https://www.sidn.nl/en/nl-domain-name/complaining-about-a-domain-name
[72] https://www.sidnlabs.nl/downloads/6tIo0U3dqydRSP781LYgDP/3c1bea3394648c44e5ea155f7e3f0887/Counterfighting_Counterfeit_detecting_and_taking_down_fraudulent_webshops_at_a_ccTLD.pdf
[73] https://www.dk-hostmaster.dk/en/how-complain-about-website-content
[74] https://www.dk-hostmaster.dk/en/issues-security-or-public-interest
[75] https://www.domaeneklager.dk/en

DIFO (and the University of Copenhagen) sponsored a research article on domain registries and website content published in 2018 that can be accessed here.

Sweden

Much like DENIC, SIDN and DK Hostmaster, The Swedish Internet Foundation also provides a number of links and suggested ways of addressing illegal activities online and shares knowledge and collaborates with organizations such as the Police and the Crime Prevention Council. The Foundation also provides a list of entities that it recommends registrants not to visit or deal with. For registrants or others who have been a victim of questionable business practices in relation to domain names, or want to report suspicious holder information, there is an email address to contact the abuse function.[76]

One of the organisations that SIF points to is the Swedish Consumer Agency that has a webpage on how to identify fake shops online.

The Swedish Internet Foundation also "focuses on spreading education and knowledge to adults in Sweden. Part of the material is about IT security from an ordinary person's perspective - how do I create strong passwords, how do I avoid being phished and are there any problems with using an open wifi?" This extensive material and dedicated site can accessed at http://internetkunskap.se/ (in Swedish only). The Foundation also makes its experts available to answer questions etc.[77]

Similarly, SIF, along the Swedish Media Council and the Swedish newspaper Metro, has developed a website on disinformation called "Fake/Fact".[78]

Japan

The only mention on the JPRS website is an email address for communicating on abuse matters. JPNIC has a page on Abuse and Spam Issues but notes that "Since our role is just allocating/assigning IP addresses, please inquire the ISP for the user of the IP address that you are looking for."[79]

South Africa

ZACR has an anti-abuse and take-down policy in which it lists a number of types of abusive practices for which a domain could be suspended, etc., including: Phishing, pharming, fraudulant websites, wilfull distribution of malware, malicious fast flux hosting, botnet command and control, spam, distribution of child pornography, illegal

[76] https://internetstiftelsen.se/en/how-to-register-a-domain-name/questionable-methods/
[77] https://internetstiftelsen.se/en/press/
[78] https://sharingsweden.se/toolkits/introducing-source-criticism-classroom/
[79] https://www.nic.ad.jp/en/abuse.html

access to other computers or networks.[80] ZACR also makes clear that it will "ZACR will make every attempt to adhere to the procedure recorded in its Complaints Management Policy and Procedure Document to address complaints pertaining to abusive practice(s) but also reserves the right to take immediate action if the integrity and stability of its domain name management system is imminent or where harm to the greater Internet user community is significant or imminent, with or without notice to the relevant registrar, reseller and/or registrant." There is also an email address to contact ZACR re abuse. One of the challenges the ccTLD manager and registry are struggling with currently are fake government websites under co.za.[81]

Additional

A number of the ccTLDs provide dispute resolution mechanisms. The European Union Intellectual Property Office published a comparative case study on alternative resolution systems for domain name disputes in 2018. Both .nl and .dk are featured. SIDN's can be found here.

[80] https://www.registry.net.za/downloads/u/ZACR_Takedown_Policy.pdf
[81] https://www.itweb.co.za/content/eDZQ58MVbxLMzXy2

Security issues

How do the policies of the ccTLDs address security issues?

The sub-questions included:

- Are policies technology-neutral or do they incentivise the promotion of security products (such as DNSSEC) by registrars and the adoption of security products by registrants?
- What policies are there on DNS abuse?
- What security policies are there, in addition to the approach of validating a registrant's details?
- Are there misspelling policies to address issues such as typosquatting?

Overview

Security is the most pressing concern for ccTLDs – their reputations as managers of the country code domains and the reliability and stability of their operations are paramount. Services and tools such as DNSSEC, anycast and server diversity, among others, are part of a ccTLD's arsenal - in addition to more tailored services often developed by the ccTLDs themselves. In recognition that security is also a shared responsibility, a number of the ccTLDs offer courses and other educational materials to both inform registrants and the broader public. ccTLDs have a number of tools to address DNS abuse, not least of which are their Terms of Service agreements.

Sweden on DNSSEC and technology neutral policies

In September 2005, the Swedish Internet Foundation was the first TLD in the world to sign their zone with DNSSEC and launched a complete DNSSEC service in February 2007, also a global first.[82] SIF's DNSSEC service is offered by many registrars for both .se and .nu, and it also provides a tool to help registrants determine if their domain is using DNSSEC or not. SIF's DNSSEC Practice Statement – a document of security practices and provisions that are related to the operation of DNSSEC in the Swedish top-level domain .se. – can be found here. The Foundation also provides a guide for DNSSEC deployment in municipalities and similar organisations here. Searching on the EUrid registrar database revealed two Danish registries offering DNSSEC: team.blue and one.com.

[82] https://internetstiftelsen.se/en/tech/dnssec-the-path-to-a-secure-domain/

SIF is also actively promoting anycast for registrars, emphasizing its network of 13 physical nodes around the globe.

Predictability is also a key element in security. SIF provides a schedule for maintenance work that is accessible here.

Sweden on DNS abuse

When addressing DNS abuse, SIF refers to its "Questionable methods" page and provides various points of contact and suggestions as well as an e-mail address for contacting the ccTLD. Further, and as noted elsewhere, under its Terms and Conditions of Registration, SIF retains the right to deactivate or deregister the Domain Name "if the Domain Name, or the use thereof, clearly violates Swedish legislation or statutes...."

Germany on DNSSEC and technology neutral policies

DENIC's registration system handles around 1 million transactions a month, and DENIC name servers, located across the globe, respond to 6 billion queries a day. As they say: "We operate an important component of the Internet infrastructure. ... Our systems must be very powerful, but also highly secure, since they have to be reliably available at any time." DENIC uses 24/7 monitoring, 11 globally distributed servers in DNS anycast system, and redundant infrastructure with two data centers, one in Frankfurt, the other in Amsterdam.

DENIC promotes its anycast system to other TLD registries and registrars through DENIC Services[83], along with DENICdirect which provides a domain name registration service (noting that "that we will not provide you with any additional Internet services when you make use of the DENICdirect service. So you will neither receive any web space, nor any email addresses nor any name service") and Data Escrow services, as one of only two accredited by ICANN as one of two designated escrow agents (DEA) for registrars worldwide.

DENIC's announced DNSSEC launch occurred in May 2011 and is now offered as an optional security feature.[84] FAQs about DNSSEC can be found here. DENIC also provides a manual if there is a change of provider for a DNSSEC-signed domain. DENIC provides DNSSEC domain statistics here. Searching on the EUrid registrar database reveals 13 that offer DNSSEC services.

[83] https://www.denic-services.de/en/
[84] https://www.denic.de/en/know-how/dnssec/

Germany on DNS abuse

With regard to DNS abuse generally, DENIC has, as noted elsewhere, stated that it "does not check the contents and/or legality of domains; responsibility for any infringement of rights resides entirely with the holder of the domain concerned." This said, DENIC has created a tool that can be used by registrants or others who feel that their rights have been infringed by a domain, called a DISPUTE entry. With regard to typosquatting, in a decision issued of January 22, 2014, the German Federal Court of Justice addressed the legality of typosquatting.[85]

It is also worth noting DENIC's Domain Terms and conditions for the conditions under which DENIC may terminate a contract:

> § 7 Termination
>
> (1) ... DENIC is only permitted to terminate the contract on substantial grounds. These grounds include, in particular, any case in which:
>
> a) The domain itself includes a manifestly illegal statement;
>
> d) The registration of the domain for the Domain Holder manifestly infringes the rights of others or is otherwise illegal, regardless of the specific use made of it;
>
> Despite the breadth of applicability that this termination clause provides, questions have been raised about its practical implementation[86] (note: article dating from 2015).

Netherlands on DNSSEC and technology neutral policies

SIDN actively promotes the use of DNSSEC[87], along with a range of additional security enhancing products and services, some developed by SIDN itself.

DNSSEC received a major boost in 2012, when the Dutch Standardisation Forum, an agency of the Ministry of Economic Affairs and the Ministry of the Interior, added DNSSEC (and DKIM) to a so-called 'use-or-explain' list. This means – according to SIDN's DNSSEC FAQ[88] - that "all (semi-) government organisations have since been more or less obliged to secure their domains and systems using DNSSEC. In practical

---

[85] https://www.whitecase.com/publications/article/german-federal-court-justice-decides-deletion-unused-domains-and-typosquatting

[86] https://www.spamhaus.org/news/article/724/ongoing-abuse-problems-at-nic.at-and-denic

[87] The DNSSEC Policy and Practice Statement can be found here.

[88] https://www.sidn.nl/en/faq/dnssec

terms, all relevant standards on the 'use-or-explain' list have to be included in tender specifications for government contracts worth more than 50,000 euros, unless there are good reasons for their non-inclusion. Consequently, the implementation of DNSSEC is normally an integral feature of public sector IT infrastructure upgrade projects." This requirement may become mandatory when the Dutch Digital Government Act becomes law. For more on the state of play in DNSSEC deployment in government and municipalities see here.

Netherlands on DNS abuse

SIDN identifies DNS abuse as threats such as DDOS attacks, dictionary attacks designed to find attractive domain names, and DNS amplification attacks, among others.[89] It manages such threats, in part, much like other ccTLDs; it identifies a number of ways of reducing DDoS attacks, noting its network of anycast nodes, and refers parties to the Dutch website of the National Cyber Security Centre.

In "What do we do if we detect abuse?" SIDN outlines how it approaches such threats – including immediately notifying the owner of the network where the abuse is coming from. If the threat is serious and the responsiveness of the network operator insufficient, SIDN will filter or block traffic.

SIDN has also set up Abuse204.nl ('abuse to zero for .nl'), a programme through which the ccTLD works with registrars to address malware and phishing and "to make .nl domain names unattractive to criminals as we possibly can". More information can be found here.

Netherlands on typosquatting

SIDN highlights the dangers of typosquatting, noting that "SIDN's Domain Name Surveillance Service alerts you whenever a domain name is registered that is very similar to your domain name or company name. Read more about DBS." The service alerts the user to lookalike .nl domain names before they are active on the internet, sending notification about registrations under top-level domains, including .com and .org, within 24 hours.

Netherlands other security work

SIDN is also active in the development of security related products and services that contribute to internet security, providing a number of security related services – including DBS above - that can be found here. These range from website security, to domain name protection, to a registry lock type service. An example is CyberSterk a service that makes "e-security clear and understandable" through monitoring "your website and your company network, identifying both serious and minor risks".

[89] https://www.sidn.nl/en/internet-security/dns-abuse

CyberSterk is a product of SIDN Business B.V., part of SIDN.[90] The launch "brochure" can be found here.

Additional security related publications and research from SIDN are available here.

Denmark on DNSSEC and technology neutral policies

As with other ccTLDs, DK Hostmaster emphasizes its own security readiness and importance of Internet security more broadly. Its goal is to "provide stable and reliable operations as well as the highest level of security and service, aligned to the day-to-day realities of our customers – which perpetually pose new challenges." It does so recommending that its customers use DNSSEC and DMARC to protect domain names against hacking and other forms of IT crime. DK Hostmaster also provides a tool for the registrant to manage DNSSEC via a self-service portal. Other services include the Very Important Domain service which uses a three person security check process for making changes to a domain name.

Recognizing that "no system is 100 per cent secure" DK Hostmaster also has a tool to encourage responsible disclosure by third parties of vulnerabilities in the ccTLD's systems. Much like the other ccTLDs DK Hostmaster is ISO 27001 certified, and DIFO and DKHostmaster have a common general framework for information security. Much like SIF, DKHostmaster also offers a number of educational resources including classes in security.

Denmark on typosquatting

DK Hostmaster provides a complaint tool to address typosquatting.[91] Typosquatting is also addressed in paragraph 9.1 of DK Hostmaster's Terms and Conditions and as a result there has been a steady decline in typosquatting: "To get rid of typosquatting we made stricter rules in 2010 so that we quickly could suspend or delete domain names that were typo-squatted. It worked and in the following years the number of typosquatting cases fell dramatically from around 900 cases in 2009 to approximately 200 cases in 2011. Today we have less than 100 cases of typosquatting per year."[92]

Denmark on DNS abuse

Articles 9.1 and 9.2 of DK Hostmaster's Terms and Conditions for the right to use a domain name provide the ccTLD with considerable powers to address unlawful use and DNS abuse more broadly. (Note: the relevant sections can be found in the Annex.)

[90] https://www.sidn.nl/en/product/cybersterk
[91] https://www.dk-hostmaster.dk/en/typosquatting
[92] https://www.dk-hostmaster.dk/en/news/fighting-online-crime-long-and-tough-battle-no-end-sight

(Of tangential interest but this tool allows one to assess which local municipalities are DNSSEC enabled across Scandinavia.)

Japan on DNSSEC and technology neutral policies

(Unfortunately many of the key documents related to terms and conditions and other matters of import are only available in Japanese and the author was not able to understand them.)

JPRS deployed DNSSEC in 2011.[93] Its DNNSEC Practice Statement – providing operational information about DNSSEC for the .jp zone – can be found here. Additional measures to increase security, stability and reliability of .jp included the introduction of IP anycast technology and distributing DNS servers in multiple geographical locations

Japan on DNS abuse

JPRS secured the TLD .jprs for technical and research purposes in 2015. It also announced a .jprs joint research project with ISPs to research connectivity in large-scale disaster situations, including state of emergency scenarios. More about .jprs can be found here and here. Interestingly, the .jprs TLD Registration Policies contain very specific and extensive abuse-related measures.[94]

In September 2019, JPRS secured ISO/IEC 27001:2013 certification on 25, the international standard for information security management systems (ISMS).

South Africa on DNSSEC and technology neutral policies

ZADNA (the ccTLD manager) and ZACR (the ccTLD registry) have adopted and implemented DNSSEC in a coordinated and uniform manner across the .ZA namespace, from the top level to second and third levels. This required putting in place the technical infrastructure, the development of a suitable policy framework and an awareness campaign directed at users and service providers within .za. The DNSSEC Policy and Practice Statement Framework to support DNSSEC in the .za namespace can be found here.

In 2015, ZADNA published the SLD (Second Level Domain) Technical Standards. These standards ensure that all .za SLDs comply with current best administrative and technical practices. The SLD Technical Standards set minimum technical and operation requirements that SLD Administrators/Registries must adhere to in order to

[93] https://jprs.co.jp/en/press/2011/110117.html
[94] https://nic.jprs/doc/jprs-registration-policies.pdf

become, or continue to serve as a .za SLD operator. A number of these standards relate to security including, among others, the use of DNSSEC, anycast, name server diversity, etc.

South Africa on DNS abuse

With regard to DNS abuse, ZADNA defines an abusive registration as one that takes "unfair advantage of another person's rights, or to be detrimental to, or infringing, another person's rights."[95]

ZACR's Anti-abuse and Take-down Policy is very clear on the range of issues that it considers abuse, from Phishing, to Fast Flux Hosting, to Child Pornography, and can be found here.

In its 2018 Published Policies and Procedures document for .co.za, ZACR outlines domain name abuse as follows:

> 14.1 The administrator will apply a level of verification on domain name registrations, to ensure that the domain name itself may not be used for:
>
> 14.1.1 Potentially spoofing local governmental institutions;
>
> 14.1.2 Inciting hate--speech or hate--crimes;
>
> 14.1.3 Distribution of child pornography; and
>
> 14.1.4 Distribution of malware.
>
> 14.2 Pursuant to clause 14.1 above, if a domain name registration is identified by the system as potentially abusive at the time of registration, the administrator will initiate domain name takedown proceedings in accordance with its Takedown Policy, available on the administrator's website.

[95] https://www.zadna.org.za/faq/domain-disputes/what-is-an-abusive-registration/

Annex

This annex is provided by the author as a way to include some interesting resources or developments in the ccTLD space that is out of scope for this research paper. These are included as they touch upon a number of key issues for ccTLDs and may provide additional "food for thought"

Additional resources – topics of potential interest:

- Internet governance – resources and background on current issues
- Code of Conduct for employees – Swedish Internet Foundation (full text)
- Unlawful use of a domain name – DK Hostmaster's terms and conditions (excerpt – in particular sections 9.2 and 9.3)

Internet governance

DENIC's extensive and useful Internet Governance portal:

https://www.denic.de/en/whats-new/news/article/denic-informationsplattform-ig-radar-macht-internet-governance-prozesse-verstaendlich/

On DNSSEC and state authorities in DK:

https://www.dk-hostmaster.dk/en/news/dnssec-domain-names-all-state-authorities

On Fake webshops in NL:

https://www.sidn.nl/en/news-and-blogs/nearly-4500-fake-webshops-taken-down-in-2019-following-detection-by-SIDN

Questions as a part of consultation on DNS abuse and the role of the

ccTLD/registry in DK:

https://www.dk-hostmaster.dk/en/news/written-hearing-regarding-role-difo-fight-against-online-crime

New administrative order for .dk:

https://www.dk-hostmaster.dk/en/news/new-administrative-order-dk

On illegal content and free expression in SE:

https://internetstiftelsen.se/en/who-takes-responsibility-for-content-online/

ccTLD code of conduct

SIF's rights-based code of conduct for employees:
https://internetstiftelsen.se/en/we-are-the-swedish-internet-foundation/code-of-conduct/

Code of conduct

The Swedish Internet Foundation's mission is to promote stability in the Swedish internet infrastructure as well as promote the spread of knowledge about the internet and electronic communication. We ensure proper conduct while conducting this mission by following this code.

The code is based on the ten principles of the UN's Global Compact. It supplements and summarizes The Swedish Internet Foundation's different policies, employee handbook and governing documents on a comprehensive level. If local, national or international law apply stricter demands than the code of conduct, these shall be followed.

The code applies to all employees regardless of employment status. We ask that all employees read and accept the regulations and apply them in all The Swedish Internet Foundation's activities. Employees are encouraged to take their own initiative to promote sustainability in the workplace. The Swedish Internet Foundation's managers are responsible for disseminating information about the code well as ensuring compliance. Suspected violation of the code must be reported to the nearest supervisor.

The code is also designed to ensure compliance in the The Swedish Internet Foundation's supplier chain. Thus, the Foundation's suppliers and their subcontractors are also covered by the code. Violation of the code entitles

The Swedish Internet Foundation to follow up through visits to suppliers and possible termination of the contract.

Human Rights

All activities should follow the guidelines of international conventions concerning basic human rights. Use of slave or child labour is completely unacceptable. The Swedish Internet Foundation also works to exclude the presence of controversial minerals in our business or supply chain.

Employees and working environment

We are convinced that different ethnic backgrounds and genders strengthen our business and we strive towards equality and diversity. The Swedish Internet Foundation does not allow any form of discrimination based on gender identity, ethnicity, nationality, religion, age, physical characteristics, sexual orientation, association or political affiliation, and similar grounds. The right to freedom of association and collective bargaining shall be recognized and respected. Every employee has the right to a fair, living wage, equal pay for equal work and regular paid vacation.

The Swedish Internet Foundation will always work for a mentally and physically healthy and safe working environment. We shall offer a workload that enables balance between work and free time. Employees shall feel that work is a developmental experience and that they have the opportunity to influence their work assignments.

Anti corruption

We act transparently, honestly and businesslike in all partnerships.

The Swedish Internet Foundation's and its employees covered by this code are expected to comply with all national and international regulations to prevent, discover and handle corruption.

Employees must refrain from acts and non-acts that involve fraud, extortion, money laundering and cartel activity. It is not allowed to request, accept of offer bribes, regardless of method, purpose and design. Benefits may only be exchanged if the process is transparent and for the creation and maintenance of a business relationship. Employees must actively promote and contribute to investigations of violations against this code of conduct.

Business decisions shall always be made with the company's best interests in mind. Transactions may not be carried out with family members, friends or people with whom other non-professional relationships exist. The Swedish Internet Foundation's employees can never use their position or influence in any way other than supporting the company's interests. If such a business arrangement or other corruption risk is identified, the grandfather principle is applied for approval of the contractor. If that is not possible, the four eyes principle shall be applied. To avoid conflict of interest, permanent employees are not to work outside of The Swedish Internet Foundation without informing their immediate supervisor of the undertaking.

Environmental responsibility

Every activity's environmental impact shall be considered when making a decision and The Swedish Internet Foundation applies the precautionary principle. We strive to use the most energy effective and environmentally friendly technology, as well as support their development. The Swedish Internet Foundation is working to reduce environmentally hazardous emissions, energy consumption and environmental impact on our immediate surroundings. Products should preferably be made of renewable, raw materials or recycled material and not use more resources or energy than necessary. They must also be easy to maintain and repair and be recyclable. We always keep all waste to a minimum. With recycling of electronic waste, both social and environmental aspects are taken into account in the choice of recycling method. When choosing energy providers and means of transport, alternatives with low environmental impact shall be prioritized.

Privacy and information

The Swedish Internet Foundation shall maintain the highest possible technical and organizational security level in order to protect critical operations as well as sensitive and personal information. Policies and rules regarding the handling of information shall be followed and extreme caution shall be observed in all electronic communication. The protection of life, health and privacy are prioritized when working with information security.

Unlawful use of a domain name

DK Hostmaster's Terms and Conditions for the use of a .dk domain name and in particular the conditions under which a domain name may be suspended.
https://www.dk-hostmaster.dk/en/terms#uretmassig

9. Unlawful use of a Domain Name

9.1 DK Hostmaster may suspend a Domain Name if:

- There is an obvious risk that the spelling or typing errors of internet users when they type an URL in an address bar are used to create confusion with a different almost identical Domain Name and thereby generate traffic on their own website,

- The Registrant of the Domain Name that is exploited in the case of confusion submits a notification,
- The Domain Name that is exploited in the case of confusion and the notified Domain Name are active in relation to the public, for example for the operation of a website,
- The notified Domain Name is registered at a later time than the notifier had his/her Domain name registered,
- The Registrant of the notified Domain Name does not have relevant trademark rights or rights to names or other distinctive marks or any other technical reason to make use of the Domain Name, and
- The Registrant of the notified Domain Name and/or a legal or natural person who is closely related to the Registrant has registered at least two other Domain Names with a corresponding obvious risk of confusion as mentioned above.

DK Hostmaster will not make a decision on suspension of the notified Domain Name until the Registrant of the Domain Name has had an opportunity to make a statement in the case.

The Registrant of the notified Domain Name gets a deadline of 72 hours to make a statement. The deadline is calculated from the time when DK Hostmaster sends the notification to the Registrant with a request for the Registrant to make a statement.

Suspension of the Domain Name is maintained for four weeks or if the decision on suspension is brought before the Complaints Board for Domain Names until the decision of the Board in the case.

After the expiry of the suspension period, DK Hostmaster deletes the notified Domain Name unless the notifier has prior to this requested DK Hostmaster to have the Domain Name transferred.

If the same Registrant has in at least two cases had a Domain Name suspended in accordance with this clause, an Agreement on the right of use to a Domain Name will be concluded with DK Hostmaster only when the Registrant enters a code sent by DK Hostmaster in a physical letter.

9.2 DK Hostmaster may suspend a Domain Name if:

- The Domain Name is used in connection with an obvious risk of economic crime, compromising of IT equipment, for example phishing and malware distribution, and/or content of a highly offensive nature, and

- The use of the Domain Name creates a risk of confusion with the Domain Name, name, logo, trademark or other distinctive marks of another natural or legal person,
- The circumstances call for not awaiting a decision from the Complaints Board for Domain Names or the courts.

Suspension of the Domain Name is maintained for four weeks or if the decision on suspension is brought before the Complaints Board for Domain Names until the decision of the Board in the case.

After the expiry of the suspension period, DK Hostmaster deletes the Domain Name unless the Registrant has documented to DK Hostmaster that the circumstance that motivated the suspension no longer exists.

9.3 DK Hostmaster may suspend a Domain Name if:

- The Domain Name is used in connection with manifestly illegal acts or omissions that infringe substantial considerations of security or public interest, and
- The circumstances call for not awaiting a decision from the Complaints Board for Domain Names or the courts.

Suspension of the Domain Name is maintained for four weeks or, if the decision on suspension is brought before the Complaints Board for Domain Names, until the decision of the Board in the case.

After the expiry of the suspension period, DK Hostmaster deletes the Domain Name.

9.4 If the manifestly illegal act or omission is directly related to a specific Domain Name, DK Hostmaster may block the Domain Name and thereby prevent any new registration of the Domain Name.

9.5 Blocking of a Domain Name means that the Domain Name is transferred to the party who has blocked the Domain Name in accordance with these Terms and Conditions. Name servers are not connected to the Domain Name which is thereby blocked from use. A Domain Fee is not payable for a blocked Domain Name.