

Non-Commercial Stakeholder Group

Representing the interests and concerns of non-commercial Internet users in domain name policy

18 July 2022

To: Goran Marby, ICANN Chief Executive Officer
To: Maarten Botterman, Chairman of the ICANN Board of Directors
Cc: ICANN Board of Directors

Re: Submission of the Human Rights Impact Assessment for ICANN's System for Standardized Access/Disclosure (SSAD) and Operational Design Assessment (ODA) Recommendations to the ICANN Boards consideration

Dear Mr. Marby and Mr. Botterman,

The Non-Commercial Stakeholder Group writes to you in order to submit the Human Rights Impact Assessment for ICANN's System for Standardized Access/Disclosure (SSAD) and Operational Design Assessment (ODA) Recommendations to the ICANN Boards consideration.

In particular, this report addresses the following:

- 1. Whether the ODA has correctly interpreted the intent of the SSAD recommendations in the proposed implementation;*
- 2. Whether the ODA has overlooked any key aspects of the SSAD recommendations that should be factored in by the ICANN Board when it considers the recommendations;*
- 3. Its view on the concerns identified by the ICANN Board in its January 2022 letter to the GNSO Council¹⁶ and potential options that could be considered, either in the form of changes to the proposed implementation or the policy recommendations themselves, to address these concerns;*
- 4. Any other considerations that the CCWP-HR believes would help to inform the Council's deliberations and consultation with the ICANN Board.*

The document was produced by the Cross-Community Working Party on ICANN and Human Rights (CCWP-HR), a group chartered by the NCSG but open to the entire ICANN Community. The primary goal of the CCWP-HR is to provide information, facilitate dialogue, and make suggestions to ICANN Org, its Board of Directors, and the ICANN community on ways to better harmonize ICANN's policies and procedures with internationally recognized human rights laws and corporate social responsibility standards. Membership is open to any interested individual regardless of affiliation.

Important to mention that the submitted document has adopted the use of the human rights impact assessments (HRIA) methodology as proposed in the FOI-HR. This methodology has been used in the October 2019 Trial HRIA for ICANN PDPs – Final Report. And, after its production, it was broadly reviewed and endorsed by the Non-Commercial Stakeholder Group membership and Policy Committee. On that note, we trust that the CCWP-HR research, as well as its findings and recommendations, will be considered by the board in future discussions on the topic.

--

The NCSG represents the interests of non-commercial users in the formulation of Domain Name System policy within the auspices of the Generic Names Supporting Organization (GNSO). Since

Non-Commercial Stakeholder Group

Representing the interests and concerns of non-commercial Internet users in domain name policy

our inception, we have facilitated global academic and civil society engagement in support of ICANN's mission, stimulating an informed citizenry and building their understanding of relevant DNS policy issues while raising awareness of the need for ICANN to comply with applicable privacy and data protection legislation.

We thank you very much for the attention and look forward to receiving a written response to these questions along with any additional documents that could be used to clarify our questions.

Yours sincerely,

Bruna Martins dos Santos
Chair, Non-Commercial Stakeholder Group

Human Rights Impact Assessment for ICANN's System for Standardized Access/Disclosure (SSAD) and Operational Design Assessment (ODA) Recommendations

Final Report

Ephraim Percy Kenyanito
Francis Monyango

June 2022

Acknowledgements

Many individuals contributed to this endeavor, and we are grateful to all who dedicated time and energy toward making this project a success.

In particular, thanks to members of the Cross-Community Working Party on ICANN and Human Rights (CCWP-HR) and Non Commercial Stakeholder Group (NCSG) for their contributions to early versions of the HRIA methodology and Non-Commercial Stakeholder Group Policy committee and membership and individual members such as Sigi Waigumo Mwanzia, Farzaneh Badii, Mallory Knodel and Stephanie Perrin for providing comments to earlier versions of the analysis of SSAD Recommendations and its ODA Recommendations.

About the CCWP-HR

The CCWP-HR is a multistakeholder forum currently chartered as a sub-entity of the Non-Commercial Stakeholder Group (NCSG) within the Generic Name Supporting Organisation (GNSO) but remains open to the rest of the Internet Corporation for Assigned Names and Numbers (ICANN) community for research and discussion on the relationship between human rights and global Domain Name System (DNS) coordination. This is related — but not limited — to policies, procedures, and operations, with a particular focus on ICANN’s responsibility to respect human rights. The primary goal of the CCWP-HR is to provide information, facilitate dialogue, and make suggestions to ICANN Org, its Board of Directors, and the ICANN community on ways to better harmonize ICANN’s policies and procedures with internationally recognized human rights laws and corporate social responsibility standards. Membership is open to any interested individual regardless of affiliation.

About the Authors

Ephraim Percy Kenyanito is a lawyer and researcher at ARTICLE 19 where he works on censorship and business and human rights issues at the Internet infrastructure level. He is a Certified Project Management Professional (PMP), has co-chaired the CCWP-HR since June 2020, and is also an alumni member of ICANN’s fellowship program, NextGen@ICANN Program among other fellowship programs.

Francis Monyango is an attorney at law and an experienced privacy and data protection practitioner and policy researcher. He is a Certified Information Privacy Professional- Europe (CIPP/E) and he is also an alumni member of ICANN’s fellowship program, NextGen@ICANN Program among other fellowship programs.

Introduction and Background

People increasingly rely on the Internet in order to carry out their normal day-to-day activities and exercise their civil, political, economic, social and cultural rights. As a result, infrastructure technologies are increasingly essential and thus human rights are a point of tension among the actors that own, operate, and manage this infrastructure.

The Domain Name System (DNS) is an important part of the global Internet infrastructure technologies. It is the proverbial phone book of the Internet, introduced in order to simplify the mapping of Internet protocol (IP) addresses to labels or user-friendly names so that users need only to specify the label or domain names of interest (like google.com, facebook.com, etc.) in the address bar of a browser to access a website or other resource, without the need to know or remember IP addresses (such as 216.58.206.174 as one of the IPs for 'google.com').

ICANN is an international non-profit multistakeholder organization incorporated to manage the Internet's unique identifier systems and coordinate the DNS.

ICANN works with various global stakeholders to set the rules on what domain names are available on the market, who operates a domain name and who operates as a distributor of IP addresses. This subsequently translates to determining whether users are able to register a domain and build a website. ICANN's policies, to a great extent, set the standards followed by registries and registrars who subsequently determine what procedures and processes to follow for an individual or an entity to register and operate a domain. Because the DNS is so integral to the way users access and share information online, the human rights aspects of ICANN's policies are an important consideration.

While, in 2002, ICANN included in its Bylaws that its core values included: "Introducing and promoting competition in the registration of domain names where practicable and beneficial in the **public interest**,¹ the interpretation of the "public interest" was not explicitly the protection of human rights." Additionally, in 2009, ICANN included in its Affirmation of Commitments that it would "[...] ensure that the outcomes of its decision-making will reflect the **public interest** and be accountable to all stakeholders."²

¹ Bylaws for Internet Corporation for Assigned Names and Numbers, *Section 1.2*

<<https://www.icann.org/resources/pages/governance/bylaws-en/#article3>> accessed June 6, 2022

² Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names And Numbers, Section 9.1

In its Articles of Incorporation in 2016, ICANN codified that it would “[promote] the **global public interest** in the operational stability of the Internet by carrying out the mission set forth in the bylaws. [...] Such **global public interest** may be determined from time to time. Any determination of such **global public interest** shall be made by the multistakeholder community through an inclusive bottom-up multistakeholder community process³.” In 2018, ICANN included in its Bylaws that it must “[...] ensure that the bottom-up, multistakeholder policy development process is used to ascertain the **global public interest**.⁴” We appreciate the pursuit of the ‘global public interest’ principle by ICANN to ensure that the Internet remains an open, inclusive and accessible resource for all. However, we note that this principle is not accompanied by clear public interest objectives. We echo the Council of Europe’s (CoE) sentiments, which noted that ICANN’s promotion of the ‘global public interest’ must be consistent with human rights as this ‘provide(s) indicators or criteria to measure to what extent the standard of ‘serving the public interest’ has been met. Human rights provide a framework which allows stakeholders to measure whether ICANN’s decisions are taken in the global public interest. Human rights are objective and internationally agreed upon with solid reasoning to clarify and justify behaviour. They provide a workable framework for checks and balances for the accountability system of ICANN.⁵

Importantly, ICANN specifically affirmed the relevance of human rights via Section 27.2 as part of its Internet Assigned Numbers Authority (IANA) transition; in 2016, ICANN revised its Bylaws to include a high-level policy commitment to “respecting internationally recognized **human rights** as required by applicable law.⁶”

However, an additional section was simultaneously added to the Bylaws specifying that the “Human Rights Bylaw” (or, more accurately, the “Human Rights Core Value”) would have no force or effect until a framework of interpretation for human rights (FOI-HR) was developed as a consensus recommendation and approved by the ICANN

<<https://www.icann.org/resources/pages/affirmation-of-commitments-2009-09-30-en>> accessed June 6, 2022

³ Amended and Restated Articles of Incorporation of Internet Corporation for Assigned Names and Numbers <<https://www.icann.org/resources/pages/governance/articles-en>> accessed June 6, 2022

⁴ Bylaws for Internet Corporation for Assigned Names and Numbers, Section 1.2

<<https://www.icann.org/resources/pages/governance/bylaws-en/#article3>> accessed June 6, 2022

⁵ ICANN’s procedures and policies in the light of human rights, fundamental freedoms and democratic values, <<https://rm.coe.int/16806fc29c>> accessed June 6, 2022

⁶ Bylaws for Internet Corporation for Assigned Names and Numbers, Section 1.2

<<https://www.icann.org/resources/pages/governance/bylaws-en/#article3>> accessed June 6, 2022

Board. This was subsequently developed and ultimately adopted⁷ by the multistakeholder community and approved by the ICANN Board in November 2019 at ICANN 66 in Montreal, Canada.

We note that the FOI-HR states, “When developing corporate or operational policies, and executing its operations, ICANN the organization should take the Human Rights Core Value into account. In order to do so ICANN the organization should propose a framework to the community, which should include multistakeholder involvement in its development, and regular review...”⁸ and, “...ICANN’s Mission, Commitments and Core Values, including the Human Rights Core Value, should be taken into account by the SOs and ACs, and ICANN the organization when considering policy matters. The Board will need to take into account ICANN’s Mission, Commitments and Core Values, including the Human Rights Core Value, in considering all matters before the Board, which also includes advice given by the GAC...”⁹

The inclusion of the “global public interest” in ICANN’s Articles of Incorporation and the operationalisation of human rights as part of ICANN’s Core Values have pivotal implications for strengthening ICANN’s accountability to its stakeholders and the global Internet community, as part of its policy development processes.

We note that the ICANN Board has taken into account the above commitments made by the ICANN community, in the recent past, and subsequently the Board has made three crucial decisions in consideration of the global public interest. The first was the ICANN Board’s rejection of the sale of the “.org” domain registry to Ethos Capital in 2020.¹⁰ Despite there being a lack of consensus within the NCSG on this rejection, this was a notable use of the global public interest framework by the ICANN Board¹¹. The

⁷ 07 Nov 2019 Approved Board Resolutions | Regular Meeting of the ICANN Board

<<https://www.icann.org/resources/board-material/resolutions-2019-11-07-en#2.c>> accessed June 6, 2022

⁸ Annex 3 – Human Rights Framework of Interpretation (HR-FOI) Final Report and Recommendations pp. 10

<<https://www.icann.org/en/system/files/files/ccwg-acct-ws2-annex-3-hr-foi-final-recs-27mar18-en.pdf>> accessed June 6, 2022

⁹ Annex 3 – Human Rights Framework of Interpretation (HR-FOI) Final Report and Recommendations pp. 10

<<https://www.icann.org/en/system/files/files/ccwg-acct-ws2-annex-3-hr-foi-final-recs-27mar18-en.pdf>> accessed June 6, 2022

¹⁰ ICANN: the .org decision shows backbone, but what next for internet reform?

<<https://www.article19.org/resources/icann-the-org-decision-shows-backbone-but-what-next-for-internet-reform/>> accessed June 5, 2022

¹¹ ICANN Board stated, “On the whole, the ICANN Board determines that the **public interest** is better served in withholding consent as a result of various factors that create unacceptable uncertainty over the future of the third largest gTLD registry.” 30 Apr 2020 Approved Board Resolutions | Special Meeting of

second was the ICANN CEO's response to reject Ukraine's request to block Russian Internet domains in 2022.¹² Third, the Board has also included the operationalisation of ICANN's global public interest commitment as part of ICANN Board Operational Priorities for Fiscal Year 2022 and this is important as Human Rights are very key to Global Public Interest as expressed in the CoE report above.¹³

As defined in the 'Terminology and Definitions' section of the report, the System for Standardized Access/Disclosure (SSAD) is 'the overall suite of parties and parts that make up the request, review, and disclosure system. It is an overall amalgamation of systems, not one specific system.'¹⁴ In summary, the SSAD is a centralised *request* protocol proposed for non-public gTLD registration data, based on the GNSO Council's EPDP Phase 2 Report.

On 25 January 2022, ICANN Org published the inaugural Operational Design Assessment (**ODA**), as an outcome of the Operational Design Phase (**ODP**) for the SSAD. As noted in the report, the ODA is intended to 'aid the ICANN Board in its consideration of GNSO policy recommendations as a result of the EPDP Phase 2 work.'¹⁵ Further, the ODA is intended to guide the ICANN Board regarding the assessment, implementation and adoption of consensus policy recommendations developed by ICANN's multistakeholder community, the GNSO. Under the ODP for the SSAD, the ODA provided input into its design, resource requirements, the SSAD build, necessary timelines, and implementation considerations, including risks.

We note that the System for Standardized Access/Disclosure (SSAD) Policy Development Process (PDP) is the first PDP to complete an Operational Design Assessment (ODA) since the formal inclusion of global public interest and human rights considerations into ICANN processes. Hence, this report by the CCWP-HR analyses the Final Report of the Temporary Specification for gTLD Registration Data

the ICANN Board <<https://www.icann.org/resources/board-material/resolutions-2020-04-30-en>> accessed June 5, 2022

¹² ICANN: Human rights law calls for an open Internet at a time of war <<https://www.article19.org/resources/icann-human-rights-law-calls-for-an-open-internet-at-a-time-of-war/>> accessed June 5, 2022

¹³ Chair's Blog: ICANN Board Operational Priorities for Fiscal Year 2022 <<https://www.icann.org/en/blogs/details/chairs-blog-icann-board-operational-priorities-for-fiscal-year-2022-21-10-2021-en>> accessed June 5, 2022

¹⁴ System for Standardized Access/Disclosure (SSAD) Operational Design Assessment (ODA), pp 14 <<https://www.icann.org/en/system/files/files/ssad-oda-25jan22-en.pdf>> accessed 6 June 2022

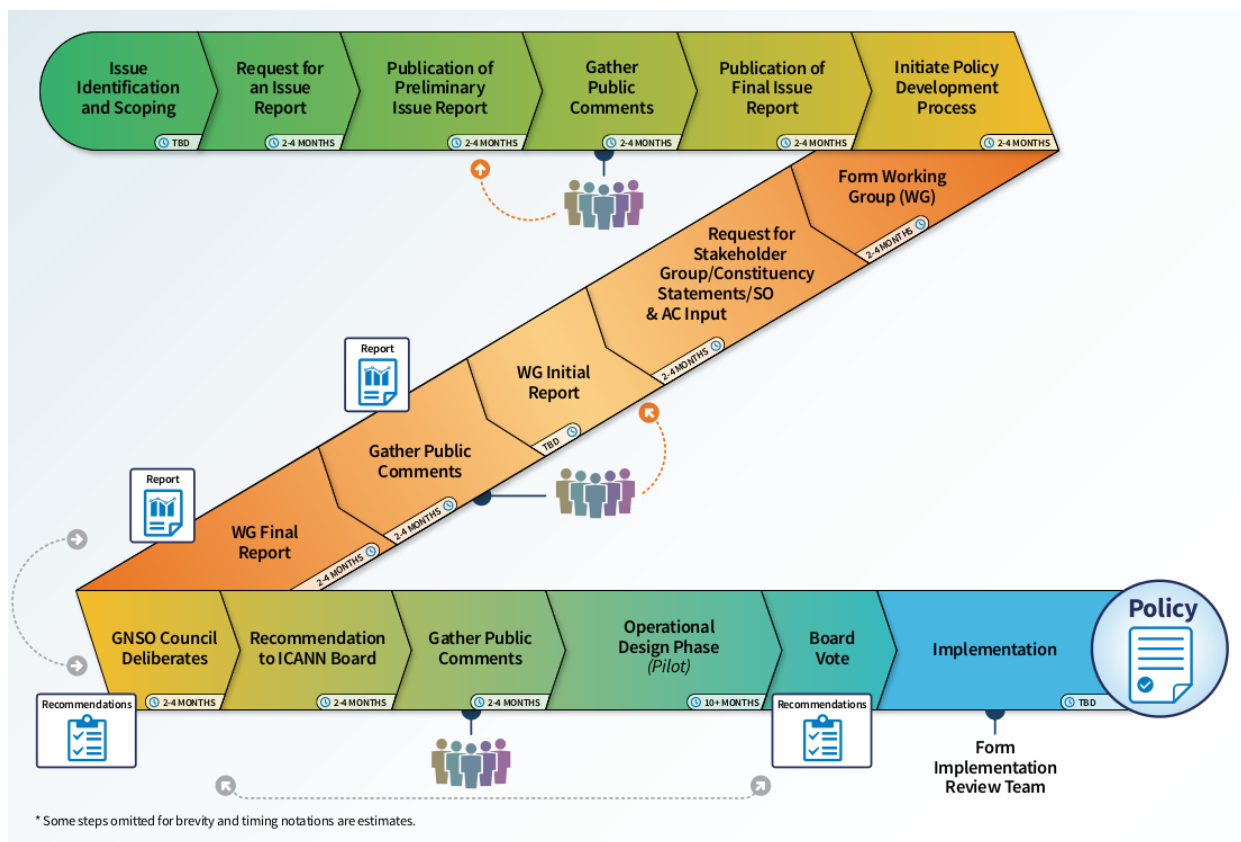
¹⁵ System for Standardized Access/Disclosure (SSAD) Operational Design Assessment (ODA), pp 6 <<https://www.icann.org/en/system/files/files/ssad-oda-25jan22-en.pdf>> accessed 6 June 2022

Phase 2 Expedited Policy Development Process (EPDP Phase 2 Report) and System for Standardized Access/Disclosure (SSAD) Operational Design Assessment (ODA) Report against the Articles of Incorporation, the Core Values and the Bylaws that address the global public interest and human rights.

In particular, this report addresses the following:

1. Whether the ODA has correctly interpreted the intent of the SSAD recommendations in the proposed implementation;
2. Whether the ODA has overlooked any key aspects of the SSAD recommendations that should be factored in by the ICANN Board when it considers the recommendations;
3. Its view on the concerns identified by the ICANN Board in its January 2022 letter to the GNSO Council¹⁶ and potential options that could be considered, either in the form of changes to the proposed implementation or the policy recommendations themselves, to address these concerns;
4. Any other considerations that the CCWP-HR believes would help to inform the Council's deliberations and consultation with the ICANN Board.

¹⁶ Letter from Botterman to Fouquart
<<https://www.icann.org/en/system/files/correspondence/botterman-to-fouquart-24jan22-en.pdf>>
accessed June 5, 2022



GNSO Policy Development Process Infographic (Source GNSO Website)

It is our hope that the ICANN Board will take this report into consideration as it makes a decision regarding the next steps towards implementation of the SSAD recommendations.

Methodology

This report has adopted the use of the human rights impact assessments (HRIA) methodology as proposed in the FOI-HR. This methodology has been used in the October 2019 Trial HRIA for ICANN PDPs – Final Report.¹⁷

We note that, the FOI-HR requires that various Supporting Organizations and Advisory Committees that comprise the ICANN community should be responsible for developing their own policies and frameworks to fulfill the Human Rights Core Value. However, the

¹⁷ October 2019 Trial HRIA for ICANN PDPs – Final Report
<https://icannhumanrights.net/wp-content/uploads/2019/10/Trial-HRIA-for-ICANN-PDPs-Final-Report-October-2019.pdf> accessed June 5, 2022

FOI-HR suggests HRIAs as a potential means of incorporating human rights considerations into policy development processes. HRIAs are rooted in the international human rights framework and used increasingly by companies, governments, and civil society alike as a tool to document a broader range of actual and potential impacts as part of a larger system of due diligence.

In response to the acknowledged agreement from stakeholders to make room for the flexible evolution of the SSAD system towards automation, through the adoption of a “hybrid” rather than centralized model¹⁸, we refer to the CoE’s report which advocates for the performance of a ‘Human Rights, Democracy, and Rule of Law Impact Assessment of AI applications’ (**HRDRIA**).¹⁹ The model proposed by the CoE calls for the incorporation of human rights considerations into the development or deployment of AI applications, guided by clearly defined criteria. This HRDRIA, where deemed necessary, will enable an assessment of potential human rights risks or violations posed by the SSAD system, giving further effect to the fulfillment of the Human Rights Core Value.

Therefore, this report uses the Comprehensive HRIA format²⁰, which was developed by the CCWP-HR in 2019, as it provides the opportunity for stakeholders with divergent positions and opinions to engage constructively through the collection and comparison of empirical evidence, anecdotes, and general observations. This report will provide the completed HRIA as an annex at the end of the report.

Second, extensive desk research was also undertaken in compiling the final report to not just identify applicable legal instruments but also review relevant cases with a view to understanding what is legal, feasible, permissible and acceptable within the confines of ICANN’s Articles of Incorporation, the Core Values and the Bylaws.

HRIA Findings

¹⁸ Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process, *pp.* 126

<<https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf>> accessed July 7, 2022

¹⁹ Human Rights, Democracy and Rule of Law Impact Assessment of AI systems

<<https://rm.coe.int/cahai-pdg-2021-05-2768-0229-3507-v-1/1680a291a3>> accessed July 7, 2022

²⁰ Human Rights Impact Assessment for ICANN PDPs – “Comprehensive Model” (January 2019 version) <<https://docs.google.com/spreadsheets/d/1WRHPWPtaK8Xc2IXtfA3MVOcprHsVVA9M6J8eUQH5UyA/e/dit?usp=sharing>> accessed June 5, 2022

General Comments and Summary

On 26 January 2022, ICANN published the ODA Recommendations, which seek to implement the EPDP Phase 2 Report. This was in response to a request from the ICANN Board for the ODA in its March 2021 resolution.²¹

We note that the EPDP Phase 2 Report attempts to propose a system that would govern the availability of WHOIS data, the conditions to access the data, and to somehow simplify the identification of requestors, if not authenticate them. Additionally, the ODA Recommendations attempt to further describe how the EPDP Phase 2 Recommendations would be implemented and provide practical guidance that is interpreted from the EPDP Phase 2 Report.

In January 2022, the ICANN Board sent a further letter²² to the GNSO Council seeking to understand if the ODA Recommendations had correctly interpreted the EPDP Phase 2 Report; with the following questions:

- a. Whether the ODA has correctly interpreted the intent of the SSAD recommendations in the proposed implementation;
- b. Whether the ODA has overlooked any key aspects of the SSAD recommendations that should be factored in by the ICANN Board when it considers the recommendations;
- c. Its view on the concerns identified by the ICANN Board and potential options that could be considered, either in the form of changes to the proposed implementation or the policy recommendations themselves, to address these concerns (note, these are expected to be high level suggestions at this stage);
- d. Any other aspects that help inform the Council's deliberations and consultation with the ICANN Board.

²¹ ICANN Board Resolution, March 2021, <<https://www.icann.org/resources/board-material/resolutions-2021-03-25-en#2.c>> accessed June 5, 2022

²² Letter from Botterman to Fouquart <<https://www.icann.org/en/system/files/correspondence/botterman-to-fouquart-24jan22-en.pdf>> accessed June 5, 2022

Our analysis shows that, despite being well-intentioned, the ODA Report, to an extent, misunderstands the EPDP Phase 2. This is also reflected in the April 2022 letter from the GNSO Council to ICANN Board.²³ In addition, the ODA Recommendations are greatly influenced by the failure of EPDP Phase 2 Recommendations to fully consider the human rights implications of the recommendations. We note that in some instances there are no clear accountability mechanisms in case of data breaches and little to no involvement of the registrants whose data would be accessed using the SSAD system.

CCWP-HR therefore urges the ICANN Board to consider the recommendations below, which would help align the EPDP Phase 2 Report and the SSAD ODA Report more closely with international human rights law and best practices.

EPDP Main report

Recommendation #1: Accreditation

While we welcome the definition and establishment of a single accreditation authority, which would be managed by ICANN and tasked with the verification, issuance, and ongoing management of identity credentials and signed assertions, we note that this is a possible single point of failure. The concept of a single accreditation authority for the management of any kind of global resource can carry with it certain risks of corruption and co-optation, precisely because there are no alternatives. Such risks can easily allow for illegal data breaches that would be detrimental to registrants.

To this end, we submit that the accreditation provisions in the final report must incorporate stronger safeguards, including enabling the creation of multiple accreditation authorities and setting operational expectations for all accreditation authorities in accordance with Article 3 ('Transparency') and Section 27 ('Human Rights') of the ICANN Bylaws.

As proposed under section 1.3.3 of the EPDP Main Report, ICANN should extensively examine potential human rights risks, including risks related to privacy and data protection, and any rights associated with criminal procedures.

Any reliance on external third party providers to handle the accreditation process, or parts thereof, despite the existence of oversight mechanisms, may jeopardize domestic

²³ Status Update EPDP Phase 2 & Review of ODA

<<https://www.icann.org/en/system/files/correspondence/fouquart-to-botterman-27apr22-en.pdf>>
accessed June 5, 2022

legal rights, and attendant liability of any players responsible for data breach or faulty legal procedure. In this regard, we recognize the potential benefits of an ICANN managed central authority. We also recognize that if there were significant volume, it would be sensible to outsource the function (on the condition that all contracts with third party providers include explicit human rights protections and compliance requirements). However, this is a central point of failure, attracts significant liability, and the rights of ICANN's clients, the Registered Name Holders or data subjects, have not been adequately analysed and safeguarded.

On the topic of registration data disclosure, we reiterate that a proper balance between the need for access to information and privacy and data protection must be struck by the registrar, registry or the central gateway manager, as applicable, when making authorisation decisions. Critically, these decisions must be guided by the guidance under Recital 47, GDPR which provides that while a controller's legitimate interests 'may provide a legal basis for processing,' this is subject to a data subject's overriding interests and fundamental rights and freedoms' and must further consider 'the reasonable expectations of data subjects based on their relationship with the controller.'²⁴

Notably, when relying on legitimate interest, the registrar, registry or the central gateway manager, as applicable, must consider 'whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.'²⁵ Where the data subject has no reasonable expectation of further processing, the registrar, registry or the central gateway manager, as applicable, must note that their interests may be overridden by the interests and fundamental rights of the data subject.

We appreciate that the draft EPDP Team Phase 2 Final Report under Section 1.4.10 places an obligation on the accreditation authority to report publicly and regularly, which is further expounded in recommendation #17 on reporting. We recommend that the reporting requirements under Section 1.4.10 further include a requirement for the authority to provide a rationale and supporting documentation whenever it approves, renews, denies or revokes accreditations, including a comprehensive description of any standard(s), including human rights considerations, that have been relied upon by

²⁴ GDPR, Recital 47, <<https://gdpr-info.eu/art-5-gdpr/>> accessed July 7, 2022

²⁵ Ibid.

the authority to make its decision.²⁶ We commend the inclusion of a ‘non-exhaustive list of examples’ for the revocation of user accreditation by the Accreditation Authority, within the context of the SSAD, under Section 1.5.1 of the draft EPDP Team Phase 2 Final Report. These include ‘the accredited user’s violation of any applicable safeguards or terms of service, 2) a change in affiliation of the accredited user, 3) violation of data retention/destruction requirements or 4) where prerequisites for accreditation no longer exist.’ To ensure the standardised application of pre-approved conditions for revocation, we propose that the report include a provision for ICANN Org to develop and publish a clear list of revocation conditions to guide the Accreditation Authority, which should be updated on a bi-annual basis to reflect learning experiences from the deployment of the SSAD system, changes in the legal framework, e.g., for data protection and privacy, amongst others.

Recommendation #3: Criteria and Content of Requests

We acknowledge that, as proposed under Recommendation #3, it is critical to standardize the criteria and content of requests to enable authorisation decisions for data requests. However, we propose that this recommendation be expanded to explicitly require requestors’ to respect and adhere to purpose, necessity and storage limitations as set under international standards, including the General Data Protection Regulation (GDPR) and the International Covenant on Civil and Political Rights (ICCPR).

We concur with the Registries Stakeholder Group’s concerns (expressed under Registries Stakeholder Group Statement on EPDP Phase II Final Report, pp. 137) and reiterate that explicit safeguards must be put in place to mitigate and address ‘risks to a registrant’s personal data,’²⁷ including instances of data misuse, such as unauthorized or unethical use of data, and the secondary processing of personal data, unless expressly permitted under the GDPR.

Placing an explicit requirement on requestors’ to adhere to the purpose limitation under Article 5 of the GDPR will ensure that data is ‘collected for specified, explicit and legitimate purposes.’²⁸ Notably, even where the purpose limitation has been satisfied, any disclosed data provided to requestors’ must be limited to what is strictly required

²⁶ The CCWP-HR is aware that transparency reportings may be complicated by legislated protections from disclosure, e.g., under national security laws.

²⁷ Registries Stakeholder Group Statement on EPDP Phase II Final Report, pp. 137

<<https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf>> accessed June 5, 2022

²⁸ GDPR, Article 5 (1) (b) <<https://gdpr-info.eu/art-5-gdpr/>> accessed June 5, 2022

‘and not further processed in a manner that is incompatible with those purposes.’ The relevance of the purpose-specification principle is re-emphasised in numerous privacy laws and standards. Article 13, principle 3 of the African Union Convention on Cyber Security and Personal Data Protection states that, “...data collection shall be undertaken for specific, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes...”²⁹ Additionally, the Organisation for Economic Co-operation and Development’s ‘Use Limitation Principle’ specifies that “Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.”³⁰ This means that when someone requests data for example to be able to investigate intellectual property violations, the same data should not be used for direct marketing to the registrants.

Further, we note that the ‘good faith affirmation’ requirement under section 3.2.4 falls far below the required data protection and privacy standards under Articles 5 and 17 of the GDPR and the ICCPR respectively, noting that the EPDP must *ensure* compliance with international privacy and data protection standards. Therefore, we recommend that the Implementation Review Team and the GNSO Standing Committee improve the recommendation by replacing this with the well-established principles for necessity and proportionality, data minimisation, lawfulness, fairness and transparency and integrity and confidentiality.³¹

Recommendation #5: Response Requirements

We commend the referral of affected parties to ‘use [of] available dispute resolution mechanisms such as courts or Data Protection Authorities’ as a means of disputing the violatory disclosure of gTLD registration data.³² However, we observe that this mechanism does not strike an appropriate balance between the access to information requirements of a third-party requester and registrants’ rights to privacy and data

²⁹ African Union Convention on Cyber Security and Personal Data Protection, Article 13
<<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>>
accessed June 5, 2022

³⁰ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Principle 10
<<https://www.oecd.org/digital/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>> accessed June 5, 2022

³¹ GDPR, Article 5 <<https://gdpr-info.eu/art-5-gdpr/>> accessed June 5, 2022

³² Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process, *Recommendation 5.4*
<<https://gns0.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf>> accessed June 5, 2022

protection, as it does not include provisions for notifying registrants when requests to access their registration data are made, so that they can appeal those requests.

We therefore recommend that a stand-alone mechanism for appeals be provided to users and registrants *before* their registration data is disclosed to third-party requesters, to ensure compliance with the principles of necessity, proportionality and the requirement for due process under international human rights law.

Recommendation #8: Contracted Party Authorization

We welcome the provision of guidelines for “disclosure requests that are routed to the Contracted Party for review,” as they explicitly require that each contracted party “...MUST review every request individually and not in bulk, regardless of whether the review is done automatically or through meaningful review and MUST NOT disclose data on the basis of accredited user category alone...”³³ Notwithstanding, we are concerned that the protections available to registrants are not on par with those offered to third-party requestors, thereby falling short of the proportionality requirement to properly balance the right of privacy and data protection vis-a-vis the desire to access information. These concerns are similar to those pointed out in Recommendation 5.

We make reference to the Court of Justice of the European Union’s (CJEU) judgment in *Google Spain*, which reaffirmed the importance of taking all circumstances, including data subjects’ reasonable expectation and interests, into account when balancing competing human rights.³⁴ Despite the focus of this ruling being on the ‘right to be forgotten’, the CJEU observed that competing rights must be considered and balanced, in accordance with the principle of proportionality, fairness and accountability. Further, we observe that these principles place an obligation on the contracted party to ensure that the disclosure of registration data is *justified* so that ‘advantages due to limiting the right are not outweighed by the disadvantages to exercise the right.’³⁵

³³ *Ibid.*, Recommendation #8

³⁴ The Court of Justice of the European Union (the CJEU), *Google Spain v AEPD & Mario Costeja Gonzalez* (2014), C-131-12. ECLI:EU:C:2014:317

<<https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=9716391>> accessed June 5, 2022

³⁵ European Data Protection Supervisor, ‘Necessity & Proportionality’

<https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en> accessed June 5, 2022

Guided by the above, we note that there is no provision of notification requirements of disclosure requests to registrants, *prior* to the disclosure of their registration data by the contracted party. Therefore, we recommend that the ‘General Requirements’ provision be expanded to include a ‘registrant notification requirement.’ This would essentially ensure that every registrant is aware whenever data is being sought about them and afforded adequate opportunity to object within legal limits such as appeals.³⁶

Further, we note that informed consent should be obtained from registrants prior to a contracted party responding to a disclosure request for registration data, ‘absent a specific legal basis, or absent a robust public interest or legal justification to do so.’³⁷ As expounded under Article 6 of the GDPR, where consent is relied on to collect data, the data should not be used or disclosed until **explicit and informed** consent from the affected party has been obtained.

Recommendation #11: SSAD Terms and Conditions

We appreciate the caveat noting that critical agreements and policies be ‘further defined during the implementation phase...to be subsequently developed and enforced by the entity responsible for the SSAD (by the ICANN organisation (“ICANN org”) or a third party that has been tasked by ICANN org to take on this enforcement function).’³⁸

To give effect to the “Human Rights Core Value” under the ICANN Bylaws, we recommend that the Implementation Review Team and the GNSO Standing Committee revise the recommendation to specifically include the completion of annual periodic HRIAs and data protection impact assessments (DPIAs) as part of critical agreements and policies.

Additionally, it is critical that any developed DPIAs and HRIAs are subjected to rigorous and regular review processes to ensure ongoing prioritization and compliance with the GDPR and international human rights standards, and provided to the public, to promote public accountability and transparency.

Recommendation #17: Reporting Requirements

³⁶ Ibid., Principle 15.4

³⁷ Ibid., *Definition of Key Terms*

³⁸ Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process, *Recommendation #11.1*

<<https://gns0.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf>> accessed June 5, 2022

We welcome the inclusion of the requirement for ‘regular public reporting on the use and functioning of the SSAD.’³⁹ CCWP-HR notes that the reporting requirements to ensure that a SSAD Status Report or dashboard is published between ‘3 - 9 months after operationalization of SSAD’ and updated on a quarterly basis will encourage predictability and transparency, promote accountability, and ensure adherence to the lawfulness principles for the processing of data.

CCWP-HR notes that reporting can be strengthened by also including the number of HRIAs and DPIAs which have been developed or reviewed, disclosing the consideration and progress of HRIA and DPIA recommendations,⁴⁰ and providing information on data breaches, at the ICANN and third -party provider levels.

Recommendation #18: Review of implementation of policy recommendations concerning SSAD using a GNSO Standing Committee

We welcome the establishment of a ‘GNSO Standing Committee’ to evaluate SSAD operational issues emerging as a result of adopted ICANN Consensus Policies and/or their implementation.’⁴¹ CCWP-HR notes that the dedication of a multi-stakeholder monitoring body tasked with evaluating operational issues, such as the GNSO Standing Committee, will promote greater accountability and oversight, and we urge that it be implemented as drafted.

ODA Report

Overall Recommendations

a. Lack of HRIAs

CCWP-HR welcomes the efforts made by ICANN to develop the ODA to “aid the ICANN Board in its consideration of GNSO policy recommendations as a result of the EPDP Phase 2 work.”⁴²

While we welcome the attempt, however not fully perfect, to incorporate protections under the EU’s GDPR and the simultaneous balancing of the right of the public and

³⁹ Ibid., *Recommendation #17.1*

⁴⁰ ARTICLE 19, ‘ICANN: one year on from its first human rights impact assessment’

<<https://www.article19.org/resources/icann-one-year-on-from-its-first-human-rights-impact-assessment/>> accessed June 6, 2022

⁴¹ Ibid., *Recommendation #18.1*

⁴² System for Standardized Access/Disclosure (SSAD) Operational Design Assessment (ODA), pp 6
<<https://www.icann.org/en/system/files/files/ssad-oda-25jan22-en.pdf>> accessed 6 June 2022

legitimate third parties to access gTLD registration data, we observe that ICANN Org’s responsibilities are global in nature, which requires the application of globally accepted human rights and data protection standards and principles, beyond the GDPR. To this end, CCWP-HR recommends that the entire EPDP and the ODA be revised to provide that countries with a poorer compliance record with human rights standards and principles or weaker data protection laws must be subject to the same international standard of human rights compliance and equal standards of data protection, as a compliance requirement under the ICANN Bylaws.

Further, we are concerned that the ODA has not comprehensively accounted for HRIAs. ICANN itself has recognised the HRIA as ‘a process to identify and prioritize the impacts an organization has on human rights, to analyze how effectively these impacts are managed by the organization and to develop actions for improvement.’⁴³

We are concerned that this failure to provide for the HRIA process, both prior to implementation of the GNSO policy recommendations and periodically during the course of full implementation of the GNSO Policy Recommendations, is a fundamental oversight that requires immediate addressing at the EPDP Report stage. Crucially, providing for HRIAs will ensure adherence with the “Human Rights Core Value” under the ICANN Bylaws and international human rights best practices.⁴⁴

To this end, we recommend that the entire ODA and the supporting EPDP be revised to include provisions for mandatory HRIAs as a compliance requirement under the ICANN Bylaws. The HRIA is a continuous compliance and due diligence process, and we recommend that the initial HRIAs be conducted and updated yearly in line with international good practice. HRIAs should focus on addressing human rights risks for all upstream and downstream ICANN stakeholders, including registrants, internal and contracted suppliers, customers and any other linked third parties, the following areas, address implementing any legal and regulatory changes in the data protection environment, and addressing any new risks affecting gTLD registration data and include all stakeholders upstream and downstream in ICANN .ie. suppliers, customers and any other linked third parties.

⁴³ Löning – Human Rights & Responsible Business, ‘Summary report of the first Human Rights Impact Assessment for the ICANN organization’
<<https://www.icann.org/en/system/files/files/summary-report-hria-15may19-en.pdf>> accessed June 6, 2022

⁴⁴ Bylaws for Internet Corporation for Assigned Names and Numbers, *Section 1.2*
<<https://www.icann.org/resources/pages/governance/bylaws-en/#article3>> accessed June 6, 2022

Further, we also recommend that HRIAs be mandated for the following actors: central gateway manager, central accreditation authority, independent auditor, SSAD misuse investigator, systems developer (if different than the operator), customer service operators (if vendors do not offer support functions), and public relations service providers.⁴⁵

b. Lack of Sufficient Public Comment Opportunities

We welcome the efforts to promote transparency and community engagement, as explained under Section A3.1 through ‘community updates, specific design updates and feedback requests.’⁴⁶ We also commend ICANN for affirming the significance of community input ‘prior to implementing the SSAD,’⁴⁷ and anticipate that the five- to six-year timeline provided for SSAD development and implementation will enable stakeholders to provide input as part of a robust consultation process. This should be reflected across the three proposed SSAD work phases, including Phase 1: Implementation Review Team Work, Phase 2: System Development and Implementation, and Phase 3: Ongoing Operations.

As a matter of best practice, various conditions must be met across the spectrum of the public participation process to be considered robust, inclusive and credible. This commentary outlines a few minimum conditions, and the CCWP-HR welcomes further engagement opportunities to comprehensively outline these conditions.

Firstly, a **sufficient deadline** for the public consultations must be provided to enable meaningful participation by internal and external stakeholders. While we are pleased that Phase 1: Implementation Review Team Work, is aligned with ICANN’s minimum Public Comment timeline of 40 days (4.5 weeks),⁴⁸ we recommend that stakeholders be provided with at least 3 months to provide inputs (to afford even those not actively participating in the ICANN space but interested in data protection and human rights to

⁴⁵ This list is not exhaustive.

⁴⁶ System for Standardized Access/Disclosure (SSAD) Operational Design Assessment (ODA), pp 106 <<https://www.icann.org/en/system/files/files/ssad-oda-25jan22-en.pdf>> accessed June 6, 2022

⁴⁷ System for Standardized Access/Disclosure (SSAD) Operational Design Assessment (ODA), pp 38 <<https://www.icann.org/en/system/files/files/ssad-oda-25jan22-en.pdf>> accessed June 6, 2022

⁴⁸ ICANN, ‘What is ICANN Public Comment?’

<<https://atlarge.icann.org/about/icann-public-comment#:~:text=What%20is%20ICANN%20Public%20Comment%3F%20Public%20Comment%20is,initiated%20by%20the%20ICANN%20Community%20and%20Staff%20Departments.>> accessed June 6, 2022

participate in the process) , noting the 2-year timelines proposed for this phase.⁴⁹ The International Association for Public Participation’s Core Values emphasizes that ‘[p]ublic participation **seeks out and facilitates** the involvement of those potentially affected by or interested in a decision.’⁵⁰ Based on this, This timeline will enable stakeholders, including those not actively participating in the ICANN space but interested in data protection and human rights, to scrutinize the proposed policy language for the Consensus Policy Implementation Framework and participate in the process), enable sufficient time for consultative scoping discussions between stakeholders, thus ensuring maximum impact on the final framework.

Secondly, the public consultations must be accompanied by vigorous **transparency and outreach efforts**. As a bare minimum, stakeholders inputs should be made available on a digital, publicly available, and accessible platform. Further, a publicly-available and time-bound report synthesizing public inputs should be provided to stakeholders detailing, as a bare minimum, (i) how and whether inputs/comments have been addressed by ICANN Org, (ii) how and whether inputs/comments have been incorporated into the final Framework; (iii), the consultation outcomes; and (iv) next steps.

Lastly, public consultations must be **ongoing** across the lifecycle of the SSAD’s development and implementation phases. We note with concern that Phase 2 and Phase 3 are almost exclusively supervised by ICANN, without any involvement from stakeholders, which raises accountability and transparency concerns.

We therefore recommend that the three SSAD development and implementation phases be revised to include robust public consultation processes, thereby ensuring that policy or operational issues can be addressed with the full involvement and participation of all stakeholders.

Recommendation: Executive Summary

a. Operational Readiness

While we welcome the process of outsourcing the verification and accreditation of SSAD requestors, we observe that this section does not set out a process for the

⁴⁹ Public Participation: Principles and Best Practice

<<https://www.icnl.org/wp-content/uploads/Attachment-3-Public-Participation-Principles-and-Best-practice-Eng.pdf>> accessed June 6, 2022

⁵⁰ IAP2 Federation’s Core Values for Public Participation <<https://www.iap2.org/page/corevalues>> accessed June 6, 2022

revocation of access to the centralized gTLD registration data system for contracted or designated vendors or governmental users, respectively. It is important to include criteria for revocations for those who have been found to have violated the right of privacy of innocent registrants. We also observe that no criteria exists to guide the selection or appointment of accreditation authorities, despite the nature of the data being handled by appointees/designees. Discussion of potential audit has been disappointing in terms of the frequency and thoroughness of the potential audit functions, not to mention independence of the auditors.

We appreciate the recognition in the ODA of the “security, stability, and resiliency risks... around inappropriate access to personal data processed within the SSAD.”⁵¹ Article 32 of the GDPR recognises unauthorised access and the disclosure of data as a risk that requires entities to establish “appropriate technical and organisational measures to ensure a level of security appropriate to the risk.”⁵²

Based on the foregoing, we recommend an introduction of a detailed process which outlines how access to the SSAD system will be revoked for appointees/designees whose permissions and access rights to the centralized system have been revoked by their respective organisations. We observe that the ODA provides for the development of a revocation criteria for Accredited Requestors during the implementation process, but a similar recommendation has not been provided for appointees/designees.

On the issue of the selections/appointment criteria of accreditation authorities, we recommend that a selection criteria be developed and inserted into the ODA as an annex, to ensure that human rights considerations and integrity standards are upheld, as specified under the international standard for accreditation, ISO/IEC 17011:2017 for accreditation practices. While the ‘international standard for accreditation allows flexibility in how a body may be structured... it must be structured so that it fosters and ensures certain principles of governance... including: impartiality; objectivity; non-discriminatory policies and practices; and avoidance of conflicts of interests.’⁵³

⁵¹ System for Standardized Access/Disclosure (SSAD) Operational Design Assessment (ODA), pp 9 <<https://www.icann.org/en/system/files/files/ssad-oda-25jan22-en.pdf>> accessed June 6, 2022

⁵² GDPR, Article 32 <<https://gdpr-info.eu/art-5-gdpr/>> accessed June 6, 2022

⁵³ A Guide to Opening the Door For Global Trade: Setting Up Accreditation Bodies In Developing Countries, pp 23 <https://open.unido.org/api/documents/6014364/download/accreditation_bodies_in_developing_countries.pdf> accessed 6 June 2022

Critically, these standards are integral to good governance which ‘promotes equity, stakeholder participation, pluralism, transparency, accountability and the rule of law, in a manner that is effective, efficient and enduring.’⁵⁴ At a minimum, any selected vendor or governmental users must be able to demonstrate integrity, objectivity, impartiality and accountability.

In this context, for the Accreditation Authority to adhere to the impartiality requirement, it must, as a minimum, provide a ‘documented and implemented structure that provides opportunity for effective involvement by interested parties.’⁵⁵ Further, the proposed AA must be ‘free from any political and commercial influence, even when government owned’ to demonstrate adherence to the impartiality requirements.⁵⁶ Critically, adhering to the accountability principle requires this would also include regular communication to the public about their decisions and policies and regular publication of transparency reports.

There is a great risk of the operator becoming embedded and gaining too much monopoly control of this important global function. Very little attention has been paid to contractor rotation; this needs to be addressed to avoid unfair competition.

b. Systems and Tools Needed

We are cognisant of the technical capacity requirements for the deployment of the SSAD, and understand the recommendation to outsource the development of the two SSAD systems, namely the ‘Central AA system, a web portal and API’ for data disclosures and the ‘Central Gateway System, a web portal and API’ for managing disclosure requests.⁵⁷

Firstly, we recommend that these two systems be held to the standard of open source and free software development, ideally incorporating best practice and protocols from standards bodies to aid in auditing platform changes iteratively to ensure the changes remain privacy centric. The CCWP-HR emphasises that the ability to view and audit platform changes in an ongoing way will be important to ensure they remain privacy-centric.

⁵⁴ Ibid. pp. 25.

⁵⁵ Ibid., pp. 36

⁵⁶ Ibid., pp. 17

⁵⁷ System for Standardized Access/Disclosure (SSAD) Operational Design Assessment (ODA), pp 8 <<https://www.icann.org/en/system/files/files/ssad-oda-25jan22-en.pdf>> accessed 6 June 2022

Secondly, we recommend that the deployment of the two SSAD systems be guided by the ‘data protection by design’ requirement under Article 25 of the GDPR, by implementing ‘appropriate technical and organisational measures... designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing.’⁵⁸

Lastly, we also recommend an expansion of this section to provide data subjects and other legitimate third parties with an express recognition of their requirements and rights with the section, further providing a redress mechanism where nonpublic disclosure data is exposed to security risks, such as unauthorized disclosure as envisaged under Chapter 8 of the GDPR. This consideration is based on a general right to due process, as individuals should have an opportunity to be able to be informed and be afforded the chance to seek out and access remedies..

Recommendation: Terminology and Definitions

a. SSAD Misuse Investigator

We understand the definition and role assigned to SSAD misuse investigators, which will be outsourced to a third party vendor, under Section A1.3 of the ODA. While we appreciate the rationale behind outsourcing the roles of monitoring and overseeing the SSAD to curb ‘potentially abusive behavior or practices by Requestors in the SSAD’, we recommend the introduction of public reporting and well-defined accountability structures for the appointed vendor, beyond contractual requirements, and the provision of a judicial mechanism to escalate concerns and provide redress solutions to affected parties.

As noted above, this is a possible single point of failure as the concept of a single monitoring, enforcement and compliance entity existing outside of the ICANN org structure carries risks of corruption and co-optation, precisely because there are no alternatives. Adopting our recommendation would offset this vulnerability by allowing for the public to scrutinise these decisions, including through an independent judicial mechanism, thereby strengthening transparency and accountability.

Recommendation: Section 2.2 - Other Issues

a. Timely Responses

⁵⁸ GDPR, Article 25 <<https://gdpr-info.eu/art-5-gdpr/>> accessed June 6, 2022

The CCWP-HR welcomes the high-level identification of the challenges around timely responses. In response to the observed lack of a timeline for contracted parties to approve data access requests from requestors in the Final Report, we make reference to the 30-day response timeline provided under the EU's GDPR, except for complex cases. Despite the GDPR being silent on the timeline for actual access to permitted data by third parties, we emphasise that there is no real justification for a lengthy delay in finding and releasing requested data. However, where personal data is being released to a third party, the registrar can take additional, but reasonable, time to verify the identity of the requestor, their reliability, and the strength of their claim to access the data.

We note that the data minimisation and storage limitation principles under Article 5 of the GDPR stipulate that access to data should be kept in accordance with the necessity standard, i.e., 'not retained for longer than is strictly necessary and as required to achieve the identified purpose(s),' unless exempted. Based on this, we note that strict time limits must be provided in the Final Report, following consultations with stakeholders, to ensure the integrity and security of registration data.

Recommendation: Section 3, Assessment

a. User Affiliation Verification

While we welcome the provision of a system to prevent misuse of the SSAD system, we are concerned by the proposal to apply penalties in a 'graduated' manner, noting that this may allow perpetrators to misuse the system multiple times, even deliberately so, before being barred from gaining access.

Therefore, we recommend that the Final Report be expanded to capture varying 'effective, proportionate and dissuasive'⁵⁹ penalties, ranging from administrative penalties to debarment, depending on the severity of the violation of the SSAD Terms of Reference.

b. Risks

While we welcome the identification of risks and proposals to control or mitigate the following risks related to the Central AA:- a) Incorrect identification, b) Unable to identify users, c) A user does not declare Representation or Affiliation, we firmly maintain that the terms 'abuse' or 'abusive' must be deleted from the Final Report and

⁵⁹ Ibid., *Article 84*

the ODA in their entirety. These terms are not defined under the ‘Terminology and Definitions’ section, and even where they are defined, their use enables subjective interpretation, misuse and potential broad application by third party contractors. Notably, the principle of the rule of law requires legal certainty and legality to be satisfied to prevent illegality and arbitrariness.

c. Data Protection Issues

While we welcome the reference of the GDPR and other data protection laws as integral to address legal issues, we note that the section fails to make reference to DPIAs and HRIAs. We therefore recommend that the section be expanded to incorporate the development and regular updating of DPIAs and HRIAs across the lifecycle of the SSAD system to ensure compliance with data protection laws and other relevant international human rights instruments. We welcome the recognition that DPIAs should be conducted ‘once the SSAD design has been set out in greater detail.’ We note that Article 35 of the GDPR requires DPIAs be carried out ‘prior to the processing... an assessment of the impact of the envisaged processing operations on the protection of personal data.’⁶⁰ We recommend that, during the carrying out of the DPIA, consultations with the EU Data Protection Regulator be held before processing under the SSAD system commences. Further, we recommend that any DPIAs be publicly disclosed to promote the principles of transparency and accountability.

d. Disclosure Request Process

As noted above, the role and purpose of SSAD misuse investigators is not envisioned under the EPDP Phase 2 Final Report, and it is also unclear to whom the misuse investigators will be accountable. Therefore, we recommend that amendments be introduced into the EPDP Final Report, with well-defined accountability structures and public reporting requirements for the appointed SSAD misuse investigator beyond contractual requirements. Additionally, we reiterate the concerns regarding the definition of the terms ‘misuse’ and ‘abuse’ as expressed in part b of this recommendation.

e. Issues Requiring Further Development

⁶⁰ Ibid., *Article 35*

We welcome the comment that a ‘pilot program can be a valuable addition to the SSAD implementation timeline, bringing additional insights into systems and tools implementation and operational readiness.’⁶¹

We recommend that the program be deployed for a period of 6-months to test out the salient technical and operational features of the SSAD system, examine the validity of assumptions made in the Final Report, identify and assess third party providers, including the Central Accreditation Authority, amongst others. This would enable the identification of any human rights impacts of the SSAD system, which will support the development of DPIAs and HRIAs prior to the formal deployment of the SSAD system.

f. Global Public Interest Framework

We welcome the examination of the impact of the EPDP Phase 2 recommendations on the global public interest. However, we recommend that a similar examination of the EPDP Phase 2 recommendations on human rights be conducted, noting the need to balance competing interests and rights, and bearing the need to ensure adherence to ICANN’s Human Rights Core Value.

Conclusion

CCWP-HR is grateful to have participated in this first HRIA of an ODA since the November 2019 ICANN Board approval of the framework of interpretation on human rights. (FOI-HR).

We firmly believe that there is a linkage between ICANN’s obligations to “global public interest” and its human rights obligations and would call on the ICANN Community to closely ensure that ICANN org, Board and all stakeholders are able to fulfill these two obligations through all stages of Policy Development Processes.

We welcome feedback on any aspect of this initiative and extend an open invitation for any interested individuals to get involved in the next phase of work. To become a member of the Cross-Community Working Party on ICANN and Human Rights (CCWP-HR), visit the CCWP-HR page on the ICANN Community website <<https://community.icann.org/display/gnsononcomstake/CCWP+on+ICANN+and+Human+Rights>>

⁶¹ System for Standardized Access/Disclosure (SSAD) Operational Design Assessment (ODA), pp 50 <<https://www.icann.org/en/system/files/files/ssad-oda-25jan22-en.pdf>> accessed June 6, 2022

ANNEX A

CCWP-HR Copy of HRIA on ICANN SSAD EPDP & ODP 2022

<https://docs.google.com/spreadsheets/d/1WRHPWPtaK8Xc2IXtfA3MVOcprHsVVA9M6J8eUQH5UyA/edit#gid=8463347>



Guidance for completing this ICANN Policy Development Process Human Rights Impact Assessment (PDP HRIA)

Field	Explanation	Tool Tip																					
PDP Topic	A few words to describe the broad topic being considered.	Useful for grouping and sorting.																					
Short Description	A few words describing the specific issue at hand.	Useful for quickly locating information.																					
Description	One or two sentences summarizing the issue.																						
Negative Impact Scenario(s)	<p>Negative impacts resulting from the situation described. To determine whether an adverse human rights impact has occurred or is likely to occur, one should consider:</p> <ul style="list-style-type: none"> - Substantive content of the right in question - Nature of business interaction or interference with the individual's right(s) - Causality - Experience and views of the rights-holders in question - Data and evidence collection, where possible 	Multiple impacts can be listed in bullet points, or broken out into multiple rows.																					
Impacted Groups	<p>Rights-holder groups who may be negatively impacted. Particular attention should be paid to groups that may be vulnerable to cumulative impacts, such as:</p> <ul style="list-style-type: none"> - Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders 	Multiple groups can be listed in bullet points, or broken out into multiple rows.																					
Severity of impact	<p>Severity of impact is determined by considering the scale, scope, and irremediability of the impact:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td rowspan="3" style="text-align: center; vertical-align: middle;">SCALE</td> <td>Life- or long-term health-threatening</td> <td style="text-align: center;">High</td> </tr> <tr> <td>Tangible infringement to access of basic freedoms (expression, education, livelihood, etc.)</td> <td style="text-align: center;">Medium</td> </tr> <tr> <td>Other impacts</td> <td style="text-align: center;">Low</td> </tr> <tr> <td rowspan="3" style="text-align: center; vertical-align: middle;">SCOPE</td> <td>>50% of identifiable group or >5,000 people</td> <td style="text-align: center;">High</td> </tr> <tr> <td>11-50% of identifiable group or 1,000 - 5,000 people</td> <td style="text-align: center;">Medium</td> </tr> <tr> <td><10% of identifiable group or <1,000 people</td> <td style="text-align: center;">Low</td> </tr> <tr> <td rowspan="3" style="text-align: center; vertical-align: middle;">IRREMIADIABILITY</td> <td>Impact cannot be remedied</td> <td style="text-align: center;">High</td> </tr> <tr> <td>Impact would be difficult to remediate</td> <td style="text-align: center;">Medium</td> </tr> <tr> <td>Impact can be easily remediated</td> <td style="text-align: center;">Low</td> </tr> </tbody> </table> <p><i>** While some type of numerical ranking might prove useful in the analysis of human rights impacts, it's important to remember that analysis can't rely on scoring alone and a thorough narrative description of impacts and proposed mitigation measures should always be provided.</i></p>	SCALE	Life- or long-term health-threatening	High	Tangible infringement to access of basic freedoms (expression, education, livelihood, etc.)	Medium	Other impacts	Low	SCOPE	>50% of identifiable group or >5,000 people	High	11-50% of identifiable group or 1,000 - 5,000 people	Medium	<10% of identifiable group or <1,000 people	Low	IRREMIADIABILITY	Impact cannot be remedied	High	Impact would be difficult to remediate	Medium	Impact can be easily remediated	Low	
SCALE	Life- or long-term health-threatening		High																				
	Tangible infringement to access of basic freedoms (expression, education, livelihood, etc.)		Medium																				
	Other impacts	Low																					
SCOPE	>50% of identifiable group or >5,000 people	High																					
	11-50% of identifiable group or 1,000 - 5,000 people	Medium																					
	<10% of identifiable group or <1,000 people	Low																					
IRREMIADIABILITY	Impact cannot be remedied	High																					
	Impact would be difficult to remediate	Medium																					
	Impact can be easily remediated	Low																					
Positive Impact Scenario(s)	Positive impacts may be noted, but the identification of "positive" human rights impacts is not the primary objective and should not detract from identifying and addressing adverse impacts.																						

<p>Examples of potentially Salient Human Rights</p>	<p>Individual rights and freedoms</p>	<ul style="list-style-type: none"> - Right to Privacy - Freedom of Expression / access to information - Right to effective remedy - Right to equal treatment / non-discrimination - Freedom of association - Right to Political participation - Right to Property - Right to Education - Right to Work / Fair remuneration - Right to a Fair trial 	
<p>Examples of potentially Applicable Human Rights Instruments</p>	<p>International treaties / conventions</p>	<ul style="list-style-type: none"> - Civil and Political Rights (ICCPR, 1966) - Economic, Social, and Cultural Rights (ICESCR, 1966) - Elimination of All Forms of Racial Discrimination (ICERD, 1965) - Elimination of Discrimination against Women (CEDAW, 1979) - Rights of Persons with Disabilities (CRPD, 2006) 	
	<p>International declarations</p>	<ul style="list-style-type: none"> - UN Declaration of Human Rights (1948) - Rights of the Child (1923) - Rights of Disabled Persons (1975) - Right to Development (1986) - Cultural diversity (2001) - Rights of indigenous peoples (2007) - Sexual orientation and gender diversity (2008) 	
	<p>Regional instruments</p>	<p>AFRICA</p> <ul style="list-style-type: none"> - African Charter on Human and Peoples' Rights (1981) <p>AMERICAS</p> <ul style="list-style-type: none"> - American Convention on Human Rights (1969) and its Protocols (1988 & 90) <p>EUROPE</p> <ul style="list-style-type: none"> - European Convention on Human Rights (1950) - European Social Charter (1961) and Protocols (1988, 91, & 95) - European Framework Convention for the Protection of National Minorities (1995) 	
	<p>State constitutions and legislation</p>	<p>E.g. national human rights acts</p>	
	<p>State thematic legislation</p>	<p>E.g. non-discrimination laws</p>	
<p>Summarized examples of potentially Relevant Bylaws</p>	<p>Commitments (1.2.a)</p>	<p>(iii) Respect creativity, innovation, and free flow of information</p> <p>(iv) Employ open, transparent, and bottom-up multistakeholder PDPs</p> <p>(v) Apply policies consistently, neutrally, objectively, and fairly without discriminatory treatment</p> <p>(vi) Remain accountable through mechanisms defined in Bylaws</p>	
	<p>Core Values (1.2.b)</p>	<p>(ii) Seek and support broad, informed participation reflecting functional, geographic, and cultural diversity of the internet</p> <p>(iv) Introduce and promote competition in registration of domain names</p> <p>(viii) Respecting internationally recognized human rights as required by applicable law</p>	
	<p>Discrimination (2.3)</p>	<p>CANN shall not apply its standards, policies, procedures, or practices inequitably or single out any particular party for disparate treatment unless justified by substantial and reasonable cause</p>	
	<p>Fairness (3.1)</p>	<p>ICANN and its constituent bodies shall operate to the maximum extent feasible in an open and transparent manner and consistent with procedures designed to ensure fairness</p>	

	GAC role (12.2.a)	The GAC should consider and provide advice on the activities of ICANN as they relate to concerns of governments, particularly matters where there may be an interaction between ICANN's policies and various laws and international agreements or where they may affect public policy issues.	
Recommendation	Recommendations should be geared toward mitigating any negative human rights impacts that have or are likely to occur. They should be clear, concise, and realistic, but don't necessarily have to provide details about roles or implementation, as these are things to be negotiated within the multistakeholder ICANN community.		Make sure that recommendations are easily communicated and understood!
Relevant links	Links to background information or other relevant materials from the ICANN website.		Only one link is permitted per cell.

* This is a living document for and by the multistakeholder ICANN community. Please feel free to make edits or additions.

EPDP Topic	Short Description	Description	Negative Impact Scenario(s)	Impacted Groups	Severity of Impact	Positive Impact Scenario(s)	Salient Human Rights	Applicable Human Rights Law	Potentially Relevant Bylaws	Recommendation	Relevant links
Recommendation #1. Accreditation	1.3.3: The establishment of, or selection of, an Accreditation Authority	The accreditation policy defines a single Accreditation Authority, managed by ICANN org, which is responsible for the verification, issuance, and ongoing management of both Identity Credentials and Signed Assertions.	Single point of failure: The concept of a single accreditation authority for the management of any kind of global resource can carry with it certain risks of corruption and co-optation, precisely because there are no alternatives. Such risks can easily allow for illegal data breaches that would be detrimental to registrants	- Registrants	Medium	This recommendation can ensure that ICANN has ultimate responsibility to ensure that rights are respected and promoted.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Article 3 and Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that, where ICANN outsources the functions, or parts thereof, of the accreditation authority, this is done only when it is necessary to do so, and that outsourcing in this manner is to function as an extension, rather than a substitute, of ICANN's responsibilities, and that all contracts with third party providers include explicit human rights protections and compliance requirements.	https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf
Recommendation #1. Accreditation	1.3.4: Decision to authorize disclosure of registration data	The decision to authorize disclosure of registration data, based on validation of the Identity Credential, Signed Assertions, and data as required in the recommendation concerning criteria and content of requests (Recommendation #3), will reside with the Registrar, Registry or the Central Gateway Manager, as applicable	Lack of a proper balance being struck between the right to access to information and privacy and data protection by the registrar, registry or the central gateway manager	- Registrants	Medium	This recommendation will introduce a requirement for the registrar, registry and central gateway managers to balance competing rights and comply with IHRL and ICANN Policies.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that the reporting requirements under Section 1.4.10 further include a requirement for the authority to provide a rationale and supporting documentation whenever it approves, renews, denies or revokes accreditations, including a comprehensive description of any standard(s), including human rights considerations, that have been relied upon by the authority to make its decision.	
Recommendation #1. Accreditation	1.4.10: Reporting	The Accreditation Authority MUST report publicly and on a regular basis on the number of accreditation requests received, accreditation requests approved/renewed, accreditations denied, accreditations revoked, complaints received and information about the identity providers it is working with. See also recommendation #17on reporting.	Poor accountability by accreditation authority	- Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders	Medium	This recommendation can assist to ensure a culture of transparency and accountability by the accreditation authority.	Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that the reporting requirements under Section 1.4.10 further include a requirement for the authority to provide a rationale and supporting documentation whenever it approves, renews, denies or revokes accreditations, including a comprehensive description of any standard(s), including human rights considerations, that have been relied upon by the authority to make its decision.	
Recommendation #3. Criteria and Content of Requests	All information necessary for a disclosure decision	The recommendation lacks an affirmation that data will not be misused or stored longer than necessarily required to fulfill the specific request.	Risks to a registrant's personal data: data misuse, such as unauthorized or unethical use of data, and the secondary processing of personal data.	- Registrants	Medium	This recommendation can assist to protect the rights of registrants and ensure adherence to purpose, necessity and storage limitations under the GDPR.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations. African Union Convention on Cyber Security and Personal Data Protection. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We propose that this recommendation be expanded to explicitly require requestors' to respect and adhere to purpose, necessity and storage limitations as set under international standards, including the General Data Protection Regulation (GDPR) and the International Covenant on Civil and Political Rights (ICCPR).	

* This is a living document for and by the multistakeholder ICANN community. Please feel free to make edits or additions.

EPDP Topic	Short Description	Description	Negative Impact Scenario(s)	Impacted Groups	Severity of Impact	Positive Impact Scenario(s)	Salient Human Rights	Applicable Human Rights Law	Potentially Relevant Bylaws	Recommendation	Relevant links
Recommendation #3. Criteria and Content of Requests	3.2.4: Good faith affirmation requirement	Affirmation that the request is being made in good faith and that data received (if any) will be processed lawfully and only in accordance with the purpose specified in (c);	Non-compliance with international privacy and data protection standards with risks to registrant's personal data.	- Registrants	Medium	This recommendation can assist to ensure compliance with international privacy and data protection standards.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations. African Union Convention on Cyber Security and Personal Data Protection. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that the Implementation Review Team and the GNSO Standing Committee improve the recommendation by replacing this with the well-established principles for necessity and proportionality, data minimisation, lawfulness, fairness and transparency and integrity and confidentiality.	
Recommendation #5. Response Requirements	5.4: Alert mechanism	ICANN org MUST make available an alert mechanism by which Requestors as well as data subjects whose data has been disclosed can alert ICANN org if they are of the view that disclosure or non-disclosure is the result of systemic abuse by a Contracted Party. This alert mechanism is not an appeal mechanism – to contest disclosure or non-disclosure affected parties are expected to use available dispute resolution mechanisms such as courts or Data Protection Authorities – but it should help inform ICANN Compliance of allegations of systemic failure to follow the requirements in this policy, which should trigger appropriate enforcement action.	The mechanism does not include provisions for notifying registrants when requests to access their registration data are made, so that they can appeal those requests.	- Registrants	Medium	This recommendation can assist to ensure a culture of transparency and accountability and protects the rights of registrants.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that the Implementation Review Team and the GNSO Standing Committee improve the recommendation by adding the requirements for users/registrants be allowed to appeal decisions to disclose their data	
Recommendation #8. Contracted Party Authorization.	Duties for Contracted Parties	Fails to include user notification requirements despite having section 8.5, which states, "Absent any legal requirements to the contrary, disclosure MUST NOT be refused solely for lack of any of the following: (i) a court order; (ii) a subpoena; (iii) a pending civil action; or (iv) a UDRP or URS proceeding; nor can refusal to disclose be solely based on the fact that the request is founded on alleged intellectual property infringement."	No provision of notification requirements of disclosure requests to registrants, prior to the disclosure of their registration data by the contracted party. Protections available to registrants are not on par with those offered to third-party requestors, thereby falling short of the proportionality requirement to properly balance the right of privacy and data protection vis-a-vis the right to access information.	-Registrants	Medium	This recommendation can assist to ensure that competing rights are considered and balanced, in accordance with the principle of proportionality, fairness and accountability.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that the Implementation Review Team and the GNSO Standing Committee improve the recommendation by expanding the 'General Requirements' provision to include a 'registrant notification requirement and ensure that informed consent should be obtained from registrants prior to a contracted party responding to a disclosure request for registration data, 'absent a specific legal basis, or absent a robust public interest or legal justification to do so.	
Recommendation #8. Contracted Party Authorization.	Contracted Party's assessment, as part of its substantive review	8.16.1.1. Assessment of impact. Consider the direct impact on data subjects as well as any broader possible consequences of the data processing. Consider the public interest and legitimate interests pursued by the Requestor to, for example, maintain the security and stability of the DNS. Whenever the circumstances of the disclosure request or the nature of the data to be disclosed suggest an increased risk for the data subject affected, this shall be taken into account during the decision-making.	No provision of notification requirements of disclosure requests to registrants, prior to the disclosure of their registration data by the contracted party. Protections available to registrants are not on par with those offered to third-party requestors, thereby falling short of the proportionality requirement to properly balance the right of privacy and data protection vis-a-vis the right to access information.	- Registrants	Medium	This recommendation can assist to ensure that competing rights are considered and balanced, in accordance with the principle of proportionality, fairness and accountability.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that the Implementation Review Team and the GNSO Standing Committee improve the recommendation by expanding the 'General Requirements' provision to include a 'registrant notification requirement and ensure that informed consent should be obtained from registrants prior to a contracted party responding to a disclosure request for registration data, 'absent a specific legal basis, or absent a robust public interest or legal justification to do so.	

* This is a living document for and by the multistakeholder ICANN community. Please feel free to make edits or additions.

EPDP Topic	Short Description	Description	Negative Impact Scenario(s)	Impacted Groups	Severity of impact	Positive Impact Scenario(s)	Salient Human Rights	Applicable Human Rights Law	Potentially Relevant Bylaws	Recommendation	Relevant links
Recommendation #11. SSAD Terms and Conditions	Recommendations on Terms and Conditions for SSAD	Failure to include DPIAs and HRIAs as part of recommendations	Can expose vulnerable persons during the Who-is-process and failure to give effect to "Human Rights Core Value" under the ICANN Bylaws	- Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders	Medium	This recommendation can assist to give to the "Human Rights Core Value" under the ICANN Bylaws.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that the Implementation Review Team and the GNSO Standing Committee revise the recommendation to specifically include the completion of annual periodic HRIAs and data protection impact assessments (DPIAs) as part of critical agreements and policies. Any developed DPIAs and HRIAs should be subjected to rigorous and regular review processes to ensure ongoing prioritization and compliance with the GDPR and international human rights standards, and provided to the public, to promote public accountability and transparency.	
Recommendation #17. Reporting Requirements	Regular public reporting on the use and functioning of the SSAD	17.2. No earlier than 3 months and no later than 9 months after the operationalization of SSAD, ICANN org MUST publish an SSAD Status Report or dashboard, and continue to do so on a quarterly basis	None	- Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders	Medium	This recommendation can promote greater predictability and transparency, promote accountability, and ensure adherence to the lawfulness principles for the processing of data.	Privacy	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that reporting be strengthened by including the number of HRIAs and DPIAs which have been developed or reviewed, disclosing the consideration and progress of HRIA and DPIA recommendations, and providing information on data breaches, at the ICANN and third-party provider levels.	
Recommendation #18. Review of implementation of policy recommendations concerning SSAD using a GNSO Standing Committee	The GNSO Council MUST establish a GNSO Standing Committee to evaluate SSAD operational issues emerging as a result of adopted ICANN Consensus Policies and/or their implementation.	18.1. The EPDP Team recommends that the GNSO Council MUST establish a GNSO Standing Committee to evaluate SSAD operational issues emerging as a result of adopted ICANN Consensus Policies and/or their implementation. The GNSO Standing Committee is intended to examine data being produced as a result of SSAD operations, and provide the GNSO Council with Recommendations on how best to make operational changes to the SSAD, which are strictly implementation measures, in addition to Recommendations based on reviewing the impact of existing Consensus Policies on SSAD operations.	None	- Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders	Low	This recommendation will promote greater accountability and oversight through the dedication of a multi-stakeholder monitoring body tasked with evaluating operational issues, such as the GNSO Standing Committee.	Privacy	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We welcome this section of the recommendation and urge that it is fully implemented as drafted.	

ODA Topic	Short Description	Description	Negative Impact Scenario(s)	Impacted Groups	Severity of impact	Positive Impact Scenario(s)	Salient Human Rights	Applicable Human Rights Law	Potentially Relevant Bylaws	Recommendation	Relevant links
ODA Entire recommendations	Lack of HRIAs	The entire ODP does not provide for express requirements to conduct HRIAs before implementation of SSAD operations by all actors i.e. 1. Central Gateway Manager 2. Central Accreditation Authority (Central AA) 3. Independent auditor 4. SSAD Misuse Investigator 5. System development (if different than the operator) 6. Customer service operators if vendors do not offer support functions 7. Public relations service provider for awareness campaigns about the SSAD prior to and post-launch	The ODA has not comprehensively accounted for HRIAs and will fail to adhere to the "Human Rights Core Value" under the ICANN Bylaws and international human rights best practices.	- Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders	High	This recommendation will provide for HRIAs and ensure adherence with the "Human Rights Core Value" under the ICANN Bylaws and international human rights best practices.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that the entire ODA and the supporting EPDP be revised to include provisions for mandatory HRIAs as a compliance requirement under the ICANN Bylaws. HRIAs should focus on addressing human rights risks for all upstream and downstream ICANN stakeholders, implement any legal and regulatory changes in the data protection environment, and address any new risks affecting gTLD registration data. HRIAs should also be mandated for the following actors: central gateway manager, central accreditation authority, independent auditor, SSAD misuse investigator, systems developer (if different than the operator), customer service operators (if vendors do not offer support functions), and public relations service providers.	https://www.icann.org/en/system/files/files/ssad-oda-25jan22-en.pdf
ODA Entire recommendations	Lack of public comment opportunities	The entire ODP does not provide for sufficient public consultation opportunities, including providing a sufficient deadline to enable meaningful participation by internal and external stakeholders, vigorous transparency and outreach efforts and ongoing consultations with stakeholders.	Poor accountability and transparency due to non-robust public consultation processes enabling policy changes affecting impacted groups without their involvement.	- Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders	High	This recommendation will provide for sufficient public consultation opportunities thus promoting greater accountability and participation by ICANN stakeholders.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We therefore recommend that the three SSAD development and implementation phases be revised to include robust public consultation processes, thereby ensuring that policy or operational issues can be addressed with the full involvement and participation of all stakeholders.	
Executive Summary- Assessment - Operational Readiness	Model for lawful disclosure of non-public Registration Data	Governmental users accessing SSAD would be verified by their country or territory's designated Accreditation Authority (AA). Each country or territory would set their desired methods for accreditation, including the designation of an AA. Countries and territories would be recognized if they are members or observers of the United Nations or are represented in ICANN's Governmental Advisory Committee. ICANN org considers the selection and appointment of one or more Governmental AAs as an internal matter for the respective governments to determine.	There is no clear process for the revocation of access to the centralized gTLD registration data system for contracted or designated vendors or governmental users. There is also no criteria to guide the selection or appointment of accreditation authorities, despite the nature of the data being handled by appointees/designees	- Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders	Medium	This recommendation will provide a clear process for the revocation of access to the centralized gTLD registration data system for contracted or designated vendors or governmental users.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend an introduction of a detailed process which outlines how access to the SSAD system will be revoked for appointees/designees whose permissions and access rights to the centralized system have been revoked by their respective organisations. Further, we recommend that a selection criteria be developed and inserted into the ODA as an annex, to ensure that human rights considerations and integrity standards are upheld, as specified under the international standard for accreditation, ISO/IEC 17011:2017 for accreditation practices.	

ODA Topic	Short Description	Description	Negative Impact Scenario(s)	Impacted Groups	Severity of impact	Positive Impact Scenario(s)	Salient Human Rights	Applicable Human Rights Law	Potentially Relevant Bylaws	Recommendation	Relevant links
Executive Summary- Systems and Tools Needed	Requirements related to the accuracy of registration data under the current ICANN contracts	Two systems must be built to deploy SSAD. ICANN org recommends outsourcing both. One is the Central AA system, a web portal and API that will be the point of entry for SSAD Requestors to ask for data disclosure. The second is the Central Gateway System, a web portal and API for contracted parties, Accreditation Authorities, the SSAD Misuse Investigator, and web portal administrators to manage disclosure requests. At least three existing ICANN services will need enhancements to support SSAD: the ICANN.org website, ICANN's RDAP client (lookup.icann.org), and the Naming Services portal (NSp). ICANN org assumes that a four-person insourced engineering team would handle these projects.	Poor appropriate technical and organisational measures in SSAD systems and limited due process opportunities for affected parties.	- Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders	Medium	This recommendation will give effect to the general right to due process, as individuals will have an opportunity to be able to be informed and be afforded the chance to seek out and access remedies.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that the deployment of the two SSAD systems be guided by the 'data protection by design' requirement under Article 25 of the GDPR, by implementing 'appropriate technical and organisational measures. We also recommend an expansion of this section to provide data subjects and other legitimate third parties with an express recognition of their rights, further providing a redress mechanism where nonpublic disclosure data is exposed to security risks, such as unauthorized disclosure as envisaged under Chapter 8 of the GDPR.	
Terminology and Definitions	The section introduces terminologies to be used in the Recommendations	SSAD Misuse Investigator- A function to monitor and verify potentially abusive behavior or practices by Requestors in the SSAD, as well as recommend corrective measures against abusive behavior. It is intended that this function be fulfilled by an outsourced vendor.	Possible single point of failure as the concept of a single monitoring, enforcement and compliance entity existing outside of the ICANN org structure carries risks of corruption and co-optation, precisely because there are no alternatives.	- Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders	Medium	This recommendation will offset the 'single point of failure' vulnerability by allowing for the public to scrutinise these decisions, thereby strengthening transparency and accountability.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend the introduction of public reporting and well-defined accountability structures for the appointed vendor, beyond contractual requirements.	
2.2 Other Issues- Timely Responses	The section introduces timelines for SSAD Operation	First, there is no standard duration or SLA from when the Contracted Parties approve a request to when they must allow Requestors access to the requested data. There are also no required standards within the Final Report as to the required length of time for such access. In addition, the Final Report does not provide details on how the Contracted Parties must support reexamination requests in terms of a specific SLA.	Lack of timelines also allow for requestors to keep the data for longer use once approved by Contracted Parties, with limited redress options.	- Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders	Medium	This recommendation will provide for strict timelines to ensure the application of an 'easy exercise' of the right to access and 'at reasonable intervals.' Further, it will ensure adherence to the data minimisation and storage limitation principles under the GDPR.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that the ICANN Board improve the recommendation by requesting ICANN Org and the EPDP team to redraft and provide strict time limits, following consultations with stakeholders, to ensure the integrity and security of registration data (Recital 63, GDPR) and the data minimisation and storage limitation principles (Article 5, GDPR).	
3.1.1.2.2 User Affiliation Verification	The section introduces requirements to verify SSAD users and differentiates between legal and natural persons	Legal Persons within the system would be renewed (re-verified) every five years. Users who misuse the system will be subject to graduated penalties and such penalties may extend to users who share the same Affiliation.	The proposal to apply penalties in a 'graduated' manner is problematic and may allow perpetrators to misuse the system multiple times, even deliberately so, before being barred from gaining access.	- Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders	Medium	This recommendation will apply 'effective, proportionate and dissuasive' penalties to prevent the misuse of the system.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that the Final Report be expanded to capture varying 'effective, proportionate and dissuasive' penalties, ranging from administrative penalties to debarment, depending on the severity of the violation of the SSAD Terms of Reference.	

ODA Topic	Short Description	Description	Negative Impact Scenario(s)	Impacted Groups	Severity of impact	Positive Impact Scenario(s)	Salient Human Rights	Applicable Human Rights Law	Potentially Relevant Bylaws	Recommendation	Relevant links
3.1.1.4 Risks	The section introduces a term "potentially abusive"	Contracted Parties can notify ICANN org of an abusive or potentially abusive user.	The terms 'abuse' or 'abusive' are not defined under the 'Terminology and Definitions' section. Even where they are defined, their use enables subjective interpretation, misuse and potential broad application by third party contractors.	<ul style="list-style-type: none"> - Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders 	High	This recommendation will give effect to the principle of the rule of law requiring legal certainty and legality to be satisfied to prevent illegality and arbitrariness.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that the ICANN Board improve the recommendation by requesting ICANN Org and the EPDP team to delete the terms 'abuse' or 'abusive' from the Final Report and the ODA in their entirety.	
3.1.3.2 Data Protection Issues	The section outlines principles that would govern SSAD	The SSAD must be built with "privacy by design" and "privacy by default" principles in mind. This means that data must be processed with the highest data protection principles (for example, only processing data that is necessary to be processed, storing such data only for as long as necessary, and limiting access to the data to those parties who require access to perform a specific SSAD function). As applied in the SSAD, this means that care must be taken to evaluate which SSAD operators require access to the data processed during SSAD accreditation, request submission, request evaluation, and, where applicable, disclosure of requested registration data. Data processed within the SSAD should also be encrypted, pseudonymized, and, where practicable, anonymized (such as through aggregation, especially where storage of such data over a longer period is required without the need to identify data subjects). Data processed within the SSAD must be deleted when it is no longer needed for the SSAD functions, including audits.	Does not make reference to DPIAs and HRIAs.	<ul style="list-style-type: none"> - Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders 	Medium	This recommendation will mandate HRIAs and DPIAs, to ensure compliance with the ICANN Bylaws and IHRL.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that the section be expanded to incorporate the development and regular updating of DPIAs and HRIAs across the lifecycle of the SSAD system to ensure compliance with data protection laws and other relevant international human rights instruments. Further, we recommend that, during the carrying out of the DPIA, consultations with the EU Data Protection Regulator be held before processing under the SSAD system commences. Lastly, we recommend that any DPIAs be publicly disclosed to promote the principles of transparency and accountability.	
3.3.1 Disclosure Request Process	The section outlines duties of the SSAD Misuse investigator	The independent SSAD Misuse Investigator will monitor and handle abusive behavior in the SSAD.	The role and purpose of SSAD misuse investigators is not envisioned under the EPDP Phase 2 Final Report. It is also unclear to whom the misuse investigators will be accountable.	<ul style="list-style-type: none"> - Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders 	Medium	This recommendation will provide well-defined accountability structures and public reporting requirements for the appointed SSAD misuse investigator beyond contractual requirements.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that amendments be introduced into the EPDP Final Report, with well-defined accountability structures and public reporting requirements for the appointed SSAD misuse investigator beyond contractual requirements.	

ODA Topic	Short Description	Description	Negative Impact Scenario(s)	Impacted Groups	Severity of impact	Positive Impact Scenario(s)	Salient Human Rights	Applicable Human Rights Law	Potentially Relevant Bylaws	Recommendation	Relevant links
3.4.3 Issues Requiring Further Development	The section recommends a pilot project to try out SSAD before rolling out the full system.	The ICANN Board's questions outlined in the Scoping Document included question 3.2.2., which asked, "Should ICANN org conduct a pilot program prior to launching the SSAD system?" ICANN org notes that a pilot program can be a valuable addition to the SSAD implementation timeline, bringing additional insights into systems and tools implementation and operational readiness. A pilot program can also reduce overall risk through the use of a prototype to reduce the unknowns for specific technical and operational concerns. That said, running a pilot program would impact the cost and timeline for the SSAD launch. ICANN org could design a program to address any specific concerns the ICANN Board may have about SSAD implementation, but to be clear, the most significant unknowns – those of demand, cost sensitivity, and actual volume – would not be discoverable via a pilot program. The ODP team would welcome additional strategic guidance from the Board and community regarding scope, acceptable levels of cost, and duration of such a pilot program	Failure to identify any human rights impacts of the SSAD system, prior to its formal deployment.	<ul style="list-style-type: none"> - Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders 	Medium	This recommendation will enable the testing of the SSAD system, prior to deployment, and enable the identification of any human rights impacts of the SSAD system.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that the program be deployed for a period of 6-months to test out the salient technical and operational features of the SSAD system, examine the validity of assumptions made in the Final Report, identify and assess third party providers, including the Central Accreditation Authority, amongst others. This would enable the identification of any human rights impacts of the SSAD system, which will support the development of DPIAs and HRIAs prior to the formal deployment of the SSAD system.	
3.10 Global Public Interest Framework	The section discusses Global Public Interest but fails to include human rights considerations	The Board's scoping document included question 3.8.1: What impact, if any, do the EPDP Phase 2 recommendations have on the global public interest as evaluated using the procedural framework that was published in June 2020 and is currently being piloted? ICANN org conducted a pilot analysis using the Global Public Interest Framework to answer this question. The analysis, which is focused on the EPDP Phase 2 recommendations for the SSAD, is found in Appendix 2. As the analysis focused on the policy recommendations and not the design for the system, design and implementation analyses are not included in this section.	Poor balancing of competing interests and rights, and bearing the need to ensure adherence to ICANN's Human Rights Core Value.	<ul style="list-style-type: none"> - Women, children, or elderly people - LGBTQ - Ethnic minorities - Religious minorities - Indigenous peoples - Persons with disabilities - Refugees or migrant workers - Human rights defenders 	Medium	This recommendation will enable a proper balancing of competing interests and rights, enabling adherence to ICANN's Human Rights Core Value.	Right to Privacy, Access to Information	International Covenant on Civil and Political Rights. General Data Protection Regulations	Section 27.2 of the ICANN Bylaws (on Human Rights) and the Framework on Interpretation for Human Rights as well as other Bylaws with an impact on human rights	We recommend that a similar examination of the EPDP Phase 2 recommendations on human rights be conducted, noting the need to balance competing interests and rights, and bearing the need to ensure adherence to ICANN's Human Rights Core Value.	