EPDP Phase 2 Policy Recommendations for Board Consideration:

NCSG Comments

March 30, 2021

About NCSG

NCSG represents the interests of non-commercial domain name registrants and end-users in the formulation of Domain Name System policy within the Generic Names Supporting Organisation (GNSO). We are proud to have individual and organizational members in over 160 countries, and as a network of academics, Internet end-users, and civil society actors, we represent a broad cross-section of the global Internet community. Since our predecessor's inception in 1999 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.

About this Public Comment Proceeding

This public comment proceeding seeks comments on the Final Report of the EPDP (https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf) including the following recommendations related to the development of the SSAD, or System for Standardized Access/Disclosure to non-public registration information:

Recommendation #1: Accreditation

Recommendation #2: Accreditation of Governmental Entities

Recommendation #3: Criteria and Content of Requests

Recommendation #4: Acknowledgment of Receipt

Recommendation #5: Response Requirements

Recommendation #6: Priority Levels

Recommendation #7: Requestor Purposes

Recommendation #8: Contracted Party Authorization

Recommendation #9: Automation of SSAD Processing

Recommendation #10: Determining Variable SLAs for response times for SSAD

Recommendation #11: SSAD Terms and Conditions

Recommendation #12: Disclosure Requirement

Recommendation #13: Query Policy

Recommendation #14: Financial Sustainability

Recommendation #15: Logging

Recommendation #16: Audits

Recommendation #17: Reporting Requirements

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

Since the coming into force of the GDPR, and the resultant Temporary Specification (https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#temp-spec) which was negotiated with the Contracted Parties, it should be noted that there has been a system of non-standardized access to non-public registration information which appears to be working.

ICANN developed a cost estimate summary, based on the assumption that it would be managing the SSAD on a totally outsourced basis, in May of 2020. (https://community.icann.org/pages/viewpage.action?pageId=134513176&preview=/134513176/134513178/SSAD%20Cost%20Estimate%20Discussion%20Paper.pdf)

The estimated recurring annual cost was 4,295,192 USD, with a start-up cost of an additional 1,664,000. USD. NCSG believes that these costs should be covered by the users of the system, through a combination of accreditation and usage fees. Depending on estimates of the number of users, which ICANN's initial study put at 20,000, these fees could be as little as $500 per year, which is easily affordable to most of the businesses who are demanding access to redacted data. Most of these companies are already paying far more to lawyers and staff to gain access via a non-standardized system. We understand that the Board is undertaking further cost estimation during the proposed "Operational Design Phase" or ODP, and we trust that the results of that more detailed exercise will be shared and discussed with the GNSO Council.

We focus our comments on the proposed recommendations, but we would like to thank ICANN staff and the leadership of the EPDP for its labours to produce these reports, and all the ancillary working documents. This has been a difficult and at times tedious negotiation of very strong stakeholder interests, and the patience and hard work of staff and leadership has been truly exemplary. The NCSG hopes that the worst is behind us, but remains committed to ensuring that we do not fall back into bad habits but rather remain committed to honouring the rights of registrants.

Comments on the Proposed Recommendations

Recommendation #1: Accreditation

> *1.The EPDP Team recommends the establishment of, or selection of, an Accreditation Authority. 1.2.The EPDP Team recommends that the Accreditation Authority establish a*

policy for accreditation of SSAD users in accordance with the recommendations outlined below….

The NCSG agrees with the detailed recommendations concerning the policy for accreditation of entities. We would note that there has been discussion of whether individuals would use the SSAD to access their own personal information. Given that most individuals, when accessing their own personal data, are most likely to be focused on financial matters and customer experience, we believe that the SSAD would be a very clumsy way to deal with data subject access requests under the GDPR or any other data protection law because it does not control any of this data. Furthermore, the Contracted Parties or their resellers are better able to authenticate individuals who are their customers. This means that Contracted Parties will have to maintain existing internal systems/personnel to respond to requests from individuals for their personal information.

We would also note that the provisions for the accreditation policy are very detailed, and cost estimates for this service may be low. Given that this is one main area where a data breach or complaints under the laws may occur, by falsely authorizing a requester, cost estimates for this function/contract may be low.

Recommendation #2: Accreditation of Governmental Entities

NCSG seeks to protect the human rights of non-commercial registrants, including free speech and the right to use domain names to exercise their rights of free speech, political speech, freedom of religion, etc. Government entities in some jurisdictions seek to harass political opponents within and outside the home country. We sincerely hope that contracted parties continue to exercise due diligence and do not provide personal/entity information relating to persecuted individuals or entities merely because the Governmental Entity has obtained accreditation. This is one of the potential slippery slopes inherent in the establishment of a centralized system: reliance of contracted parties on remote systems to ensure the rights of customers are maintained.

Recommendation #3: Criteria and Content of Requests

Generally, the detailed provisions in this section meet requirements for the gateway manager to consider, in our view. However, we would note section 3.5

3.5.Requests must be in English unless the Contracted Party that is receiving the request indicates they are also willing to receive the request and/or supporting documents in other language(s).

Supporting documents regarding legal matters are likely to be in other languages, leading to translation issues. We trust these costs have been factored into the SSAD.

Recommendation #4: Acknowledgment of Receipt

No comments.

Recommendation #5: Response Requirements

5.3 If a Requestor is of the view that its request was denied in violation of the procedural requirements of this policy, a complaint MAY be filed with ICANN Org. ICANN Org

MUST investigate complaints regarding disclosure requests under its enforcement processes.

5.4.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.

Throughout this EPDP, NCSG has commented frequently that the focus is on the "rights" of the requestor to access data. This is not a right, it is a privilege. Registered Name Holders, subjected to contractual obligations, have rights, which need to be detailed in a policy that has never managed to be published at ICANN, despite efforts in the past. These two sections of the response requirements illustrate the low priority placed on ICANN's enforcement of the rights of the individual registrants….if there is a pattern of systemic abuse in requests, then ICANN should investigate the systemic abuse of **Requestors**, as well as the sloppy handling of information requests on the part of the Contracted Parties. If we wait for the data to have been wrongfully released, the horse has left the barn.

Recommendation #6: Priority Levels

NCSG notes that there has been considerable discussion concerning reasonable response times. While we have sympathy for urgent requests where lives are in danger, or there is ongoing perpetration of malware/cyberattack, we do support the Contracted Parties' concerns about cost escalation if they are required to maintain extra staff to respond to requestors who are primarily concerned about their own financial harms, not those of the public. We trust that the language in this section reflects a reasonable compromise, but look forward to future discussion in implementation.

Recommendation #7: Requestor Purposes

No comments.

Recommendation #8: Contracted Party Authorization

This recommendation includes a very interesting subsection pertaining to the obligations of the Contracted Parties:

8.1. 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.*

As we know, automated decision making has been frowned upon in most data protection laws, and Article 22 of the GDPR basically carries over the prohibition against automated decision-making regarding an individual from the previous Directive 95/46/EC. We do think that "meaningful" should be changed to "human" to avoid confusion.

There are basically three concepts here that have been intermingled:

- Disclosure based on accredited user category alone is not permitted
- Each request for access must be reviewed individually, not in bulk
- There are two types of review, automatic and manual or human.

More clarity concerning obligations of the Contracted Parties with respect to automation appears in the next section, but this phrase casts doubt on adherence to the obligations inherent in automated processing.

Recommendation #9: Automation of SSAD Processing

There are a great many obligations here, provided in great detail. The section is silent on the obligations on Contracted Parties to inform registered name holders of the disclosure of their data. This is an omission which should be rectified by a cross reference to Recommendation 12, where these rights are described. Registrants in many instances have the right to know if their data has been requested, particularly when it comes to law enforcement requests.

One of the mandatory automated replies requires further elaboration:

> *9.4.2.The investigation of an infringement of the data protection legislation allegedly committed by ICANN/Contracted Parties affecting the registrant.*

It should be noted that the investigation must be by the authorized data protection commissioner or their representative, or a duly authorized representative of the individual whose data is the subject of the complaint.

Recommendation #10: Determining Variable SLAs for response times for SSAD

No comment.

Recommendation #11: SSAD Terms and Conditions

No comment.

Recommendation #12: Disclosure Requirement

> *12.2. Contracted Parties and the Central Gateway Manager:*
>
> *12.2.1. MUST process data in compliance with applicable law;*
>
> *12.2.2. Where required by applicable law, MUST disclose to the Registered Name Holder (data subject), on reasonable request, confirmation of the processing of personal data relating to them, noting, however, the nature of legal investigations or procedures MAY require SSAD and/or the disclosing entity to keep the nature or existence of certain requests confidential from the data subject. Confidential requests MAY be disclosed to data subjects in cooperation with the requesting entity, and in accordance with the data subject's rights under applicable law;*
>
> *12.2.3. Where required by applicable law, MUST provide mechanism under which the data subject may exercise its right to erasure, to object to automated processing of its*

personal information should this processing have a legal or similarly significant effect, and any other applicable rights;

12.2.4. MUST, in a concise, transparent, intelligible and easily accessible form, using clear and plain language, provide notice to data subjects, of the types of entities/third parties which may process their data. For the avoidance of doubt, Contracted Parties MUST provide the above-described notice to its registrant customers, and the SSAD MUST provide the above-described notice to SSAD users. For Contracted Parties, this notice MUST contain information on potential recipients of non-public registration data including, but not limited to the recipients listed in Recommendation #7 Requestor Purposes, as legally permissible. Information duties according to applicable laws may apply additionally, but the information referenced above MUST be contained as a minimum.

The notice of potential release of information should accompany annual reminders to update registration data to ensure accuracy. Many years ago, there was an effort at ICANN to produce a document of Registrants' Rights. This morphed into a document on Registrants' Obligations. It is high time that a thorough document which details registrants' rights, risks, and responsibilities is produced that will help with the onerous task of educating them on this topic.

Recommendation #13: Query Policy

Recommendation 13 deals with the actions of requestors, and provides a requirement for the gateway manager to deal with abusive requestors. Once again, the language employed here displays the bias that we have noted throughout this PDP….that Contracted Parties have "must" requirements in terms of disclosures of non-public information, whilst the requestors "may" suffer repercussions if their requests are abusive. The only clear example which merits immediate response is the use of stolen credentials; this is not only a security violation, but potentially a criminal act. Nevertheless, the language is as follows:

Implementation Guidance
13.4. Abusive behavior ***can ultimately result*** *in suspension or termination of access to the SSAD;* ***however, a graduated penalty scheme should be considered*** *in implementation.* ***There may, however, be certain instances of egregious abuse, such as counterfeiting or stealing credentials, where termination would be immediate.***

Where is the MUST language directing the gateway manager to immediately act on presentation of evidence of stolen credentials? What about other patterns of misrepresentation? Are we attempting at all to protect the rights of registrants, remembering that some releases have been recommended to be automatic at the gateway level, or does the entire responsibility of protecting the rights of registrants rest on the shoulders of the contracted parties? ICANN has a responsibility to audit and enforce adherence to data protection law and this policy. We provide an edited text as an annex, due to its length, with suggested changes in bold and footnotes deleted.

We must emphasize that taking a lenient approach with requestors who are attempting to "game" the system and get access to personal data they are not entitled to receive, could potentially lead to a finding of data breach or inadequate security controls. Criminal behaviour such as stealing credentials or identities should be reported to the appropriate authorities.

Recommendation #14: Financial Sustainability

This section is really a discussion of all the issues raised in funding an automated system. NCSG has maintained all along that users who gain disclosures from the system should be responsible for its financial support. Users who generate larger costs, such as high-scale users, should pay proportionally more than users who cause smaller portions of the cost. We certainly agree that the registered name holder MUST NOT be charged a fee in any form for third parties gaining access to his/her data. However, the section proceeds to ramble back and forth as to who can charge fees. In the ICANN ecosystem, all monies come ultimately from the registered name holders at this point, so more specificity is required here to acknowledge a new payer will be required to foot the bill for this system.

As a general observation, NCSG believes that if we can achieve a standardized and consistent application of the disclosure policy without building a new system, we should do so, This would involve leaving third party access to RNH data in the hands of the data controllers, that is, the contracted parties. If third party seekers of access are unwilling to shoulder the costs of supporting an SSAD, they are de facto telling us they do not value it enough to justify its implementation.

Recommendation #15: Logging

No comments

Recommendation #16: Audits

No comments, other than to remark that many data protection authorities have audit powers and should be encouraged to review the logs and records of the system to ensure compliance.

Recommendation #17: Reporting Requirements

No comments.

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

Given the length of time it has taken to comply with data protection law, and the difficulty in reaching consensus, the NCSG must register its concern that this proposed Standing Committee will continue to generate a hefty workload for its members, and potentially the GNSO Council and any subsequent related PDPs. In particular, this section:

> *i. Any policy or implementation topic concerning SSAD operations may be raised by a member of the GNSO Standing Committee, and shall be placed on the Committee's working agenda if seconded by at least one other 'group's' Committee member.*

While we understand the need for a low impact method of monitoring how the policy is implemented, we warn ICANN against allowing this Standing Committee to bypass the GNSO and make policy, or to re-litigate issues that were decided in the policy development process. This particular clause has the potential to keep discussions in limbo for some time, and contribute to further burnout of members. It must be monitored to ensure that it remains effective.

We will not comment at this time on issues that are still being debated in the EPDP 2a.

Conclusion

The NCSG has been calling for respecting the privacy rights of registered name holders since the earliest days of ICANN. We collaborated with the Council of Europe to bring a host of data protection experts, including then European Data Protection Supervisor Giovanni Buttarelli and the UN Special Rapporteur on Privacy Professor Joseph Cannataci to the public meeting in Copenhagen (ICANN 58, March 2017) prior to the coming into force of the GDPR. We are therefore very pleased at the progress that has been made, whilst being mindful of the fact that respect for the human rights of registered name holders remains elusive. Progress in compliance with data protection law has been driven by concerns about the financial risk of the co-controllers of the data, because of the size of the fines potentially levied as a result of the GDPR and all the other data protection legislation which is being amended to conform to that standard. Nevertheless, progress is real and we remain committed to doing our part to ensure that it continues throughout implementation.

Annex 1: Suggested language for Section 13 Query Policy

Note the reordering; changes are marked in bold.

13.1.The EPDP Team recommends that the Central Gateway Manager:

> 13.1.1. MUST monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system;
>
> **13.1.2 MUST immediately investigate complaints of the use of false, stolen or counterfeit credentials to access the system, and take immediate action to remove the access rights of the perpetrators, and recommend to the accreditation body that the abusers be investigated and de-accredited.**

NCSG comment: This offense, if it were to result in the improper disclosure of personal data, is a major breach of data protection law. Failure to respond immediately to a valid complaint from any of the parties involved in the potential release of the data would be a failure to comply with law in an area where due diligence is required. The rights of the data subjects must be a focus here.

> **13.1.3 MUST immediately investigate complaints of the following behaviour, and take action to remove the perpetrators if the complaints are justified:**
>
> **13.1.3.1. High volume automated submissions of malformed or incomplete requests.**
>
> **13.1.3.2. High volume automated duplicate requests that are frivolous, malicious or vexatious.**
>
> **13.1.3.3. Storing/delaying and sending high-volume requests causing the SSAD or other parties to fail SLA performance.**
>
> 13.1.4. MAY take measures to limit the number of requests that are submitted by the same Requestor if it is demonstrated that the requests are of an abusive nature.

13.1.5. As with other access policy violations, abusive behavior can ultimately result in suspension or termination of access to the SSAD. In the event the Central Gateway Manager makes a determination based on abuse to limit the number of requests from a Requestor, the Requestor MAY seek redress via ICANN org if it believes the determination is unjustified. For the avoidance of doubt, if the SSAD receives a high volume of requests from the same Requestor, the volume alone must not result in a de facto determination of system abuse.

13.1.6. MUST respond only to requests for a specific domain name for which non-public registration data is requested to be disclosed and MUST examine each request individually and not in bulk, regardless of whether the consideration is done automatically or through **human** review.

13.2. The EPDP Team recommends that Contracted Parties:

13.2.1. MUST NOT reject disclosure requests from SSAD on the basis of abusive behavior which has not been determined abusive by the Central Gateway Manager as described above. The Central Gateway Manager MUST provide a mechanism for Contracted Parties to report perceived abusive requestors/requests and provide a determination regarding the requestor/request within the timeframe allowed for the Contracted Party to provide a response. Alternatively, the Contracted Party shall be permitted to delay providing a response until such time that the Central Gateway Manager has reviewed the report of abuse and made a determination.

Appropriate SLAs for the Central Gateway Manager need to be set, with the needs of the Contracted Parties to get approval to ignore miscreant behaviour in mind.

13.3. No further changes to this section