System for Standardized Access/Disclosure to Non-Public Registration Data (SSAD) – Draft Responses to Charter Questions & Preliminary Recommendations

For review and discussion at the LA F2F Meeting (9-11 Sep 2019)

To facilitate the development of these proposed policy principles and preliminary recommendations, the EPDP Team developed a number of use cases to better understand the needs of third parties in requesting access to and disclosure of non-public registration data. The use cases developed covered the following categories:

- Criminal Law enforcement/national or public security
- Non-LE investigations and civil claims
- Need for redacted data for a third party to contact registrant
- Consumer protection, abuse prevention, digital service provider (DSP) and network security
- Registered Name Holder consent or contract

A template was developed to facilitate this review, detailing for each use case a number of aspects such as data elements typically required, lawful basis of the entity disclosing the data and safeguards. For further details, please see https://community.icann.org/x/-KCjBg.

At the direction of EPDP Leadership, the staff support team developed this document to serve as a starting point for the deliberations at the EPDP Team F2F meeting in Los Angeles from 9-11 September 2019. These proposed policy principles, building blocks and implementation guidance were derived from the EPDP Team's discussions and review of the use cases.

Please note that this paper aims to represent views that appeared to have been broadly shared but these do NOT represent formally agreed to EPDP Team positions. Further review and discussion during the LA F2F meeting will need to confirm whether there is support for these policy principles, building blocks and implementation guidance and if not, how these should be modified to achieve general support. The paper also identifies a number of questions that are intended to aid the EPDP Team in further detailing its intent. Where applicable, diverging positions or approaches have been documented as best as possible.

POLICY PRINCIPLES AND SSAD BUILDING BLOCKS

As a result of its deliberations on the use cases, the following policy principles and SSAD building blocks are put forward for further discussion. The proposed policy principles do not necessarily create new requirements for contracted parties, but these policy principles must be adhered to in the implementation of the policy recommendations and underpin the implementation of SSAD.

SSAD POLICY PRINCIPLES

Policy Principle #1. The objective of the SSAD is to provide a predictable, transparent and accountable mechanism for access/disclosure of non-public registration data.

Policy Principle #2. Compliance with GDPR and other applicable data protection legislations underpins the SSAD.

Policy Principle #3. The mechanism chosen to ultimately implement the SSAD must have the ability to adhere to these policy principles and recommendations.

Policy Principle #4. Requestors must comply with the requirements outlined in the policy recommendations when submitting disclosure / access requests.

Policy Principle #5. Requests must be justifiably necessary and proportionate to the legitimate interest identified in the request for disclosure. In addition, the non-public data elements requested should not be readily available through other means.

Policy Principle #6. Contracted parties must comply with the requirements outlined in the policy recommendations when receiving disclosure / access requests.

Policy Principle #7. Automated processing of SSAD requests is desirable, but only where it has been established that doing so does not negatively affect the rights of the data subject. Automation does not imply automatic disclosure / access.

Policy Principle #8. If user groups are created, being identified as part of a particular user group does not create an automatic right of disclosure or access to certain data elements (see also policy principle #6).

Policy Principle #9. [1]Each processing activity in the context of access/disclosure requires its own lawful basis, as outlined in the GDPR. Specifically, a requestor of registration data must have a lawful basis for both its receipt and any subsequent processing of the data. Separately, the controller must have a lawful basis for disclosing registration data to the requestor. The EPDP Team's work will focus on the lawful basis of the entity

[1] Charter question a2

disclosing the data's disclosure, although it is not within the EPDP Team's remit nor expertise to conclusively determine which lawful basis may apply – this will remain the responsibility of the entity disclosing the data. The requestor will be responsible for identifying its lawful bases; those determinations are not within the remit of the EPDP Team.

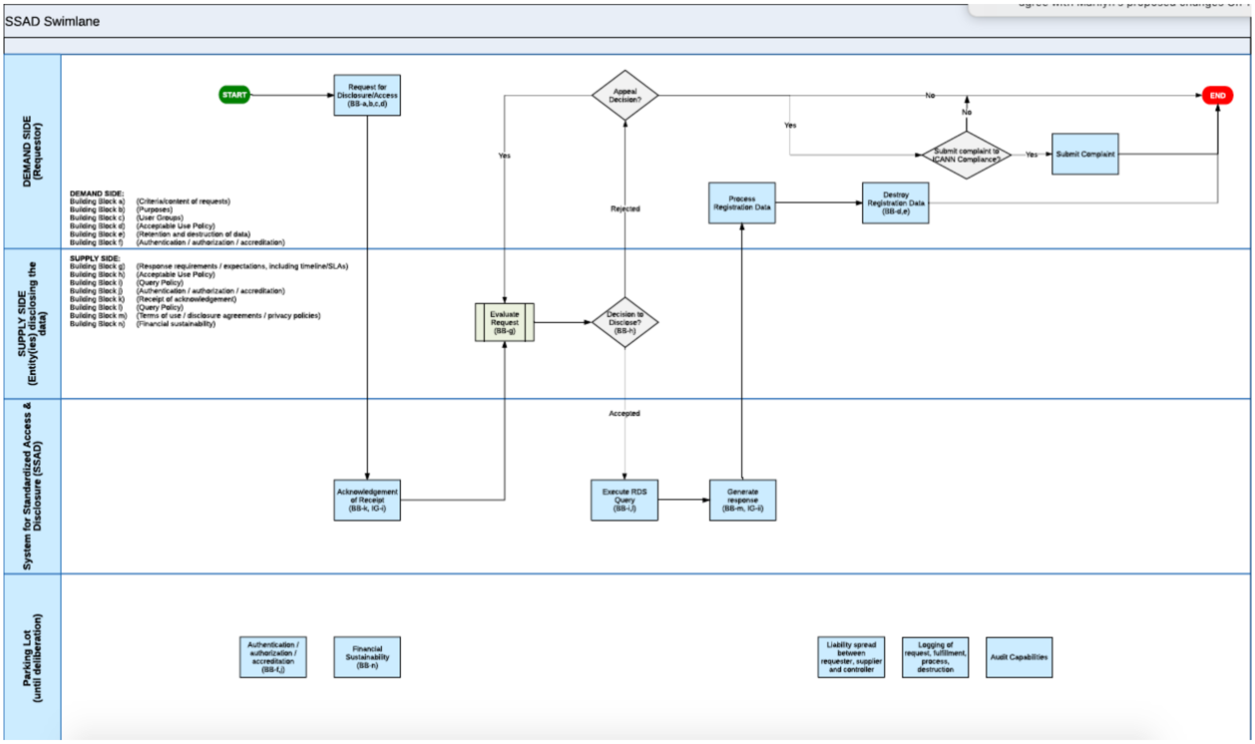
Policy Principle #10. The entity disclosing the data will remain ultimately responsible for assessing whether any disclosure or non-disclosure is in violation of any applicable laws.

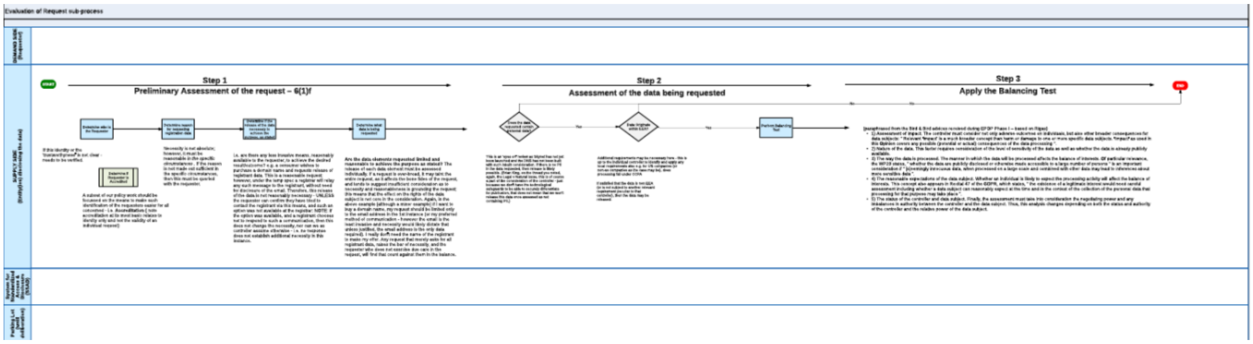
Policy Principle #11. Contracted parties are only responsible for disclosing non-public registration data for the domain names under their management.

Policy Principle #12. In order to facilitate implementation of the policy recommendations, requestors may be categorized, and these categories may be used to organize certain processes as described in the policy recommendations (e.g. accreditation, authentication).

SSAD BUILDING BLOCKS

In order to fully appreciate the different aspects of the SSAD, the following graphics aim to illustrate the different steps as well as related building blocks (which are further detailed below).


SSAD Swimlane
DEMAND SIDE (Requestor)
SUPPLY SIDE (Entity(ies) disclosing the data)
System for Standardized Access & Disclosure (SSAD)
Parking Lot (until deliberation)
START
Request for Disclosure/Access (BB-a,b,c,d)
Appeal Decision?
Yes
No
END
Submit complaint to ICANN Compliance?
Submit Complaint
Rejected
Process Registration Data
Destroy Registration Data (BB-d,e)
DEMAND SIDE:
Building Block a) (Criteria/content of requests)
Building Block b) (Purposes)
Building Block c) (User Groups)
Building Block d) (Acceptable Use Policy)
Building Block e) (Retention and destruction of data)
Building Block f) (Authentication / authorization / accreditation)
SUPPLY SIDE:
Building Block g) (Response requirements / expectations, including timeline/SLAs)
Building Block h) (Acceptable Use Policy)
Building Block i) (Query Policy)
Building Block j) (Authentication / authorization / accreditation)
Building Block k) (Receipt of acknowledgement)
Building Block l) (Query Policy)
Building Block m) (Terms of use / disclosure agreements / privacy policies)
Building Block n) (Financial sustainability)
Evaluate Request (BB-g)
Decision to Disclose? (BB-h)
Accepted
Acknowledgement of Receipt (BB-k, IG-i)
Execute RDS Query (BB-i,l)
Generate response (BB-m, IG-ii)
Authentication / authorization / accreditation (BB-f,j)
Financial Sustainability (BB-n)
Liability spread between requester, supplier and controller
Logging of request, fulfillment, process, destruction
Audit Capabilities


Evaluation of Request sub-process
DEMAND SIDE (Requestor)
SUPPLY SIDE (Entity(ies) disclosing the data)
System for Standardized Access & Disclosure (SSAD)
Parking Lot (until deliberation)
START
Step 1
Preliminary Assessment of the request – 6(1)f
Step 2
Assessment of the data being requested
Step 3
Apply the Balancing Test
Determine if Requestor is Accredited

(for full screen version, please see Annex to this paper)

DEMAND SIDE: Requestor

Building Block a) *(Criteria/content of requests[2])*
The EPDP Team recommends that, consistent with the EPDP Phase 1 recommendations, each SSAD request must include, at a minimum, the following information:

a) Identification of and information about the requestor (including, the nature/type of business entity or individual, Power of Attorney statements, where applicable and relevant);
b) Information about the legal rights of the requestor and specific rationale and/or justification for the request, (e.g. What is the basis or reason for the request; Why is it necessary for the requestor to ask for this data?);
c) Affirmation that the request is being made in good faith;
d) A list of data elements requested by the requestor and why this data is limited to the need[3];
e) Agreement to process lawfully any data received in response to the request.

Building Block b) *(Purposes[4])*
The EPDP Team recommends that requestors must be able to identify at a minimum from the following legitimate interests to request disclosure / access:

a) Criminal Law enforcement/national or public security
b) Non-LE investigations and civil claims
c) Need for redacted data for a third party to contact registrant
d) Consumer protection, abuse prevention, digital service provider (DSP) and network security
e) Registered Name Holder consent or contract

With respect to the ICANN purpose for this disclosure, the EPDP Team recommends that: [TBD]

[2] Charter question a3
[3] Charter question a5 and a6
[4] Charter question a1

Building Block c) *(User Groups[5])*

The EPDP Team recommends that requestors must be able to self-identify at a minimum from one of the following user groups:

a) Criminal Law enforcement/national or public security
b) Network operator
c) Provider of online services
d) Commercial security service
e) Non-LE investigator
f) Internet user
g) Consumer protection organization
h) Social Media Companies
i) Messaging Services
j) Search Engines
k) UDRP / URS Provider
l) Copyright owners, exclusive licensees, their attorneys or agents
m) Certificate authority
n) Registered name holder (data subject)
o) Company interested in acquiring new domain name(s)
p) Operational security practitioner
q) Anti-abuse authority
r) Digital crime investigator

Self-identifying as a certain user group does not provide any kind of automatic access / disclosure, but may facilitate the processing of the SSAD request. Each request, including those from accredited users, will need to meet the requirements as outlined in these policy principles and recommendations to ensure that it concerns a valid and legitimate request.

Building Block d) *(Acceptable Use Policy[6])*

The EPDP Team recommends that the following requirements are applicable to the requestor and must be confirmed & enforced by [TBC]:

a) Must only request data from the current RDS data set (no data about the domain name registration's history);
b) Must provide representations with each unique request for data of its corresponding purpose and legal basis for their processing which will be subject to auditing (no bulk access);
c) Must only use the data for the purpose requested;

[5] Charter question a4

[6] Charter questions c1-7

d) Must handle the data subject’s personal data in compliance with data protection laws such as GDPR;
e) Must provide representations about use of requested data which will be subject to auditing;
f) [Other]

[Additional requirements in the case of the following purpose [state purpose] are:
TBC based on review of use cases]

Building Block e) *(Retention and destruction of data)*
The EPDP Team recommends that requestors must confirm that they will store, protect and dispose of the data in accordance with any applicable requirements in relevant data protection laws such as GDPR.

Building Block f) *(Authentication / authorization / accreditation[7])*
The EPDP Team recommends that user groups interested in accreditation should self-organize and develop a proposed accreditation mechanism that is shared with the European Data Protection Board for review. Any such accreditation mechanism is expected to adhere to the following principles:

a) Must provide for a mechanism for de-accreditation in case of abuse of access / disclosure of non-public registration data;
b) Accreditation may not result in any kind of automatic access / disclosure, but it is expected to facilitate review of requests and automation, where applicable;
c) [Other]

Those wanting to be accredited must:

a) Agree to only use the data for the legitimate and lawful purpose described above;
b) If applicable, only issue disclosure requests with respect to the trademark(s) where ownership is evidenced;
c) Agree to:
    - the terms of service, in which the lawful use of data described;
    - prevent abuse of data received;
    - be subject to de-accreditation if they are found to abuse use of data;
    - maintain a register of all requests also including the respective rightsholders name (subject to audits).

Failure to abide by safeguards would affect accreditation, including the possibility of revocation.

<u>SUPPLY SIDE – Entity Disclosing The Data</u>

[7] Charter questions b1, b2 and b3

(Open questions:

- Who will be the entity (or entities) disclosing the data?
- Will there be a single access point or multiple?
- If/how can liability be reduced / shared between contracted parties, entity disclosing the data (if different from contracted parties) and requestor?)

Building Block g) *(Response requirements / expectations, including timeline/SLAs)*

Consistent with the EPDP Phase 1 recommendations, the EPDP Team recommends that [TBC]

The EPDP Team recommends that if the entity disclosing the data determines that disclosure would be in violation of applicable laws AND result in inconsistency with these policy recommendations, the entity disclosing the data must document the rationale and communicate this information to the requestor and ICANN Compliance (if requested).

If a requestor is of the view that the entity disclosing the data's response is not consistent with these policy recommendations or applicable data protection legislation, a complaint should be filed with ICANN Compliance or the relevant data protection authority.

Building Block h) *(Acceptable Use Policy[8])*

The EPDP Team recommends that the following requirements are applicable to the entity disclosing the data and must be confirmed & enforced by [TBC]:

a) Must only supply the necessary data requested by the requestor;
b) Must return current data in response to a request;
c) Must process data in compliance with data protection laws such as GDPR;
d) Must log requests;
e) Where applicable, must define and perform a balancing test before processing the data. The data subject should be able to challenge –with proper substantiation- the balancing test with rights to object and to erasure;
f) Must disclose to the Registered Name Holder (data subject), on reasonable request, confirmation of the processing of personal data relating to them, per relevant data protection laws such as GDPR;
g) Any system designed for disclosing of non-public registration data to Law Enforcement Authorities must include a mechanism for implementing the need for confidentiality for ongoing investigations.

Building Block i) *(Query Policy)*

The EPDP Team recommends that the entity disclosing the data:

[8] Charter questions c1-7

a) May take measures to limit the number of requests that are submitted by the same requestor if it is clear that the requests are not legitimate and of an abusive nature;
b) Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system, such as unjustified, high-volume automated queries;
c) [Other]

A response to an SSAD request must not include more non-public data elements than have been requested by the requestor. The response must include the public data elements related to the domain name registration.

An SSAD request meeting the requirements as outlined in these policy recommendations must be received for each domain name registration for which non-public registration is requested to be disclosed. Each such request should be examined on its own merits.

Building Block j) *(Authentication / authorization / accreditation[9])*
The EPDP Team recommends that the entity disclosing the data must:

a) Provide the ability for confirmed accreditors to confirm accredited requestors in SSAD;
b) Provide for a mechanism to report abuse by an accredited user which is relayed to the accreditation authority for handling;
c) Confirm the validity of each request;
d) [Other]

System for Standardized Access / Disclosure (SSAD)

Building Block k) *(Receipt of acknowledgement)*
The EPDP Team recommends that, consistent with the EPDP Phase 1 recommendations, the response time for acknowledging receipt of a SSAD request should be without undue delay, but not more than two (2) business days from receipt, unless shown circumstances does not make this possible.

The response should also include information about the subsequent steps as well as the timeline consistent with the recommendations outlined below.

Building Block l) *(Query Policy)*
The EPDP Team recommends the SSAD, in whatever form it eventually takes, MUST:

a) Unless otherwise required or permitted, not allow bulk access,[10] wildcard requests, reverse lookups, nor boolean search capabilities.
b) Must only return current data (no data about the domain name registration's history);
c) Must receive a specific request for every individual domain name (no bulk access[11]);

[9] Charter questions b1, b2 and b3
[10] As described in section 3.3.6 of the Registrar Accreditation Agreement
[11] As defined in section 3.3.6 of the Registrar Accreditation Agreement.

d) Must direct requests at the entity that is determined through this policy process to be responsible for the disclosure of the requested data.

Requests must only refer to current registration data (historical registration data will not be made available via this mechanism).

Building Block m) *(Terms of use / disclosure agreements / privacy policies)*
The EPDP Team recommends that [TBC]

Building Block n) *(Financial sustainability)*
The EPDP Team recommends that [TBC]

SSAD IMPLEMENTATION GUIDANCE

Implementation Guidance #i.
The EPDP Team recommends that, consistent with the preliminary recommendation that an SSAD must be received for each domain name registration for which non-public registration is requested to be disclosed, it must be possible for requestors to submit multiple requests at the same time, for example, by entering multiple domain name registrations in the same request form if the same request information applies.

Implementation Guidance #ii.
SSAD must also return the publicly-available registration data associated with the domain name registration for which a access/disclosure request has been made.