# 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)*

# *Updated version – 8 September 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 (version 27 August 2019) 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.

Subsequently, EPDP Team members were requested to provide their input to the zero draft (see <https://docs.google.com/document/d/1TKw8tOe0qgkXgBNLjVxb7l7tu20UF9t-/edit?ts=5d730234>). Based on the input received by 6 September 2019, the staff support team has updated this document to reflect questions and issues flagged which are intended to guide the discussion’s during the F2F meeting.

**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**

*Staff support team comment: Following review by EPDP Team, further determination to be made as to whether some or all should remain as ‘policy principles’ or need to be translated into policy recommendations, accompanying notes (or are not needed for the purpose of the Initial Report).*

1. The objective of the SSAD is to provide a predictable, transparent and accountable mechanism for access/disclosure of non-public registration data where such disclosure has been proven to be warranted.

*Comments / concerns / questions to be considered in relation to policy principle #1:*

* *The EPDP Team has not confirmed yet that an SSAD is required. Explicit discussion and agreement should be part of the F2F meeting.*
* *Confirm whether SSAD should only provide access/disclosure of non-public registration data or should it also return publicly available domain name registration data to a query? What would be the rationale for not allowing the return of publicly available domain name registration data?*
* *Should “to third parties with a legitimate interest and a legal basis” be added to the end of the sentence? Would that exclude certain lawful basis?*

1. The SSAD is to be designed in observance of the “privacy by design principle”. This includes Constitutional and fundamental human rights protection in addition to applicable data protection law. ~~Compliance with GDPR and other applicable data protection legislations underpins the SSAD.~~

*Comments / concerns / questions to be considered in relation to policy principle #2:*

* *SSAD must provide a flexible framework that allows those CPs to comply with GDPR and other applicable legislation. How would this policy principle need to be updated to better reflect this notion? The policy principle should embrace the concept of protecting registrants’ fundamental rights, rather than reluctantly permitting CPs to manage their risk under DP law. The text surrounding our policy must not be such that it proves embarrassing when read out in a higher Court, clearly demonstrating the reluctance to protect personal information.*

1. The mechanism chosen to ultimately implement the SSAD must have the ability to adhere to these policy principles and recommendations. *I doubt that a mechanism has the ability to adhere to policy principles and recommendations. The mechanism must be built in accordance with policy, which reflects the law and fundamental human rights (including due process). “The mechanism” cannot be an autonomous engine, there has to be a data controller behind it accepting responsibility for actions. That entity (the controller or processor as the case may be) has to have the ability, both through the mechanical engine chosen, and attendant processes and procedures, to adhere to policy.*

*Comments / concerns / questions to be considered in relation to policy principle #3:*

* *The mechanism cannot only be an ‘implementation’ choice, it needs to be made by the EPDP Team after careful consideration and factoring in the legal responsibilities that CPs have and how these may be affected by the choice of mechanism.*
* *This policy will drive the technical requirements of any future SSAD implementation. (not the other way around).*
* *We are talking about a disclosure instrument here. The instrument has limits, in terms of what it can do on behalf of data controllers/processors, to analyze requests for data, determine their eligibility, disclose and track requests, seek consent where required, provide notice to registrants where required, etc. Those limits are to be determined, from a policy perspective, after we study a number of factors:*

*Cost, affordability, who pays*

*Ability to discriminate between one requestor and another*

*Ability to sufficiently analyze a request to determine legitimacy*

*Logging, tracking, and identification of requestors*

*Audit capability, role of the auditors, (who pays)*

*Registrants’ rights management (access, correction, deletion, right to be forgotten, notification of lawful access under relevant local law)*

1. Requestors must comply with the requirements outlined in the policy recommendations when submitting disclosure / access requests.

*Comments / concerns / questions to be considered in relation to policy principle #4:*

* *More specificity will be needed that detail the expectations with regards to compliance by requestors.*

1. Requests must be justifiably necessary and proportionate to the rights of the individual in question. The legitimate interest identified in the request for disclosure must be detailed, specific, and in compliance with law. In addition, the non-public data elements requested should not be readily available through other means. (where did this come from? I do not think that law enforcement in particular should be required to seek other avenues, as they may have legitimate reasons to prefer this source of data)

*Comments / concerns / questions to be considered in relation to policy principle #5:*

* *Consider removing "justifiably" - Necessary and proportionate are legal concepts and should not be diluted. And they relate to the rights of the individual…we need more legal clarity here, it seems like we are just parroting the words in the wrong sense.*
* *Reconsider using the word ‘readily’ – DPAs have indicated that there should be no "alternative" to achieving the same outcomes by other means. Meaning if you don’t need personal data to do the job, don’t ask for it (eg many cybercrime investigations so not need PI). It does not mean shop elsewhere….(e.g. the ISPs)*
* *Consider removing “In addition, the non-public data elements requested should not be readily available through other means.” as this seems to impose a different standard than “necessary and proportionate“ under GDPR. ???? see above, not sure where we are going with this discussion*
* *Consider changing legitimate interest to lawful basis - Legitimate interest is one of several possible lawful bases for disclosure of personal data. Sigh, requestor must prove necessity. I recognize the difficulty in reflecting all the desired language in the GDPR, but would suggest that plain language may offer a way out. Requestor must demonstrate, in their requests, who they are, why they need every element of the protected data, and under what basis in law they are requesting it. I believe that focusing on the “legitimate interests” of the requestors leads us down a garden path.*
* *Proposed rewording: “"Requests must have a sound legal basis or must be justifiably necessary and proportionate to the legitimate interest identified in the request for disclosure.”*

1. Contracted parties must comply with the requirements outlined in the policy recommendations when receiving disclosure / access requests.

*Comments / concerns / questions to be considered in relation to policy principle #6:*

* *Consider adding “as long as these requirements are in compliance with applicable data privacy law.” Let’s be clear here: if the contracted parties are deemed to be the controllers, then they can be encouraged to follow this policy but at the end of the day they are still responsible and accountable for the release of data through this engine. It is up to them whether they think the policy/mechanism can be relied upon to make a competent decision in the matter of a request.*

1. 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.

*Comments / concerns / questions to be considered in relation to policy principle #7:*

* *Need to ensure that SSAD automation does not increase, in any manner, the risk of the contracted parties or to the data subjects. Which is impossible. Delete in any manner, replace with the concept of building this thing to achieve acceptable risk. This may mean manuyal processing of requests that are not straightforward.*
* *Need to clarify and be specific about the difference between “automated processing of SSAD requests” and “automatic disclosure/access.” Yup, big difference*
* *Need to define automatic, automated and automated in this context. Duplication, I hope…*
* *Consider that the issue is not whether a data subjects rights are negatively affected, but rather whether automatic processing provides a reasonable and proportionate response (per Principle #5). (cf. tbd legal advice). See above.*
* *Automated processing of SSAD requests does not guarantee automatic disclosure / access but consider also stating that it does not rule it out.*
* *Consider updating “automated processing of SSAD requests is desirable” to reflect what is allowed under GDPR by adding “but only where allowed by applicable privacy law.” There may be another law that affects registrants’ rights locally, such as consumer protection law or telecom law. I would suggest broadening references to dp law to “applicable law, particularly data protection law”*

1. 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).

*Comments / concerns / questions to be considered in relation to policy principle #8:*

* *The issue of accreditation first needs to be clarified and resolved before this principle is further considered. Accreditation must only be employed as a means to guarantee identity of applicants. This removes one big messy step for the data controller, if there are groups that will attest to the identity of their members, but that is all accreditation does or can do.*

1. [[1]](#footnote-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 ~~authorizing~~ 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. This is very unclear to me here. Obviously, we are trying to identify the policy framework under which a disclosure instrument might operate. WE are not adjudicating individual requests. However , we have done a lot of work on use cases (against the better judgement of many members….was this not to illustrate which kinds of requests might be legitimate and which might not, in order to better imagine how feasible it is to construct an automated, autonomous disclosure mechanism? WE cannot just toss all the reasons for disclosure into a black hole and say the machine with decide. The controller must decide, in accordance with this policy, and we must provide guidance that aims at best practice or highest standard, not highest acceptable risk.

*Comments / concerns / questions to be considered in relation to policy principle #9:*

* *Consider changing to a positive obligation instead of a qualifier (“Requester MUST have a lawful basis”)*
* *Consider clarifying to indicate that the category of requestor does not equate with legal basis.*
* *Instead of referring to a specific law, consider changing to "adherence to data protection principles and applicable law."*
* *Consider that any SSAD system must enable requesters to both state and back up their legal basis with facts/data/information/etc – this could be confirmed in the form of an implementation note?*
* *Consider removing the fourth sentence (“The EPDP Team’s work….”) – does it add anything?*

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

*Comments / concerns / questions to be considered in relation to policy principle #10:*

* *The EPDP Team to prioritize who the entity / entities will be.*
* *Once it is decided who the entity/ entities will be, it may not be necessary to include this principle as it is a given. I think this is far from a throw away line. Decide whether the entity is a controller or processor and map out the responsibilities and liabilities.*

1. Contracted parties are only responsible for disclosing non-public registration data for the domain names under their management. This on the other hand is a throw away line….what other scenario exists? If there are others , e.g. going through another CP because the CP managing the data is a suspected criminal, then perhaps this may not actually be true, there may be valid reasons for access shopping.

*Comments / concerns / questions to be considered in relation to policy principle #11:*

* *This seems to imply that CPs would be the entity/entities disclosing but this still needs to confirmed. However, even in a centralized model, CPs would likely disclose to entity responsible for disclosure to requestors. Following decision on who entity / entities disclosing the data, revisit this principle. Definitely have to revisit*
* *Consider updating by removing ‘non-public registration data’*

1. 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).

*Comments / concerns / questions to be considered in relation to policy principle #12:*

* *Consider updating to reflect that requests and not requestors may be categorized. Consider following three categories:1) Legal basis (for request), 2)Legal Basis for disclosure and 3) Urgency of request. yes*

*New policy principles suggested:*

*Policy Principle #NEW: Policy recommendations should not result in burdensome implementation costs to Contracted Parties, which would or could result in the shifting of these costs to registrants. These costs should be considered, especially where they will be the result of the interests of third parties who will likely bear none or little of the costs created.*

*Comments:*

* *Would adding this principle constrain the work of the EPDP Team? This is a fundamental issue, are you kidding? We are not here to restore free data services to third parties, we are here to [finally] comply with 25 year old data protection law and protest registrants’ rights. If automating it costs too much then we are not doing it!!!*
* *It may be premature to add this now and better to reconsider once the EPDP Team completes its work on the related building block? No, costs are always always always a primary policy consideration. Proceeding with all this policy work without considerings costs and who will pay is totally irresponsible.*

**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).





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

**DEMAND SIDE: Requestor**

1. *(Criteria/content of requests[[2]](#footnote-2))*

*Staff support team comment: Note, this has not been specifically discussed but is based on the EPDP Team’s recommendations developed in phase 1 of its work. Will need to be cross-checked with implementation of phase 1 recommendations.*

The EPDP Team recommends that, consistent with the EPDP Phase 1 recommendations, each SSAD request must include, at a minimum, the following information:

1. Identification of and information about the requestor (including, the nature/type of business entity or individual, Power of Attorney statements, where applicable and relevant);
2. 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?);
3. Affirmation that the request is being made in good faith; This is meaningless unless the requestor accepts liability for any malfeasance. Need identity of individual taking responsibility for the good faith request and their status in the organization.
4. A list of data elements requested by the requestor and why this data is limited to the need[[3]](#footnote-3);
5. Agreement to process lawfully any data received in response to the request.

I don’t think this is enough. Some jurisdictions may have no relevant law, or entities be above the law. Need to Specify precise obligations (e.g. destruction of data according to best practice).

*Comments / concerns / questions to be considered in relation to building block a):*

* *Does this address manual request per EPDP phase 1 rec #18 or automated request via a centralized system?*
* *Bullet d - Consider tighter language, closer to the GDPRs requirements (“A list of data elements requested by the requestor, and why this data is strictly necessary and are no broader than required").*
* *Consider adding “domain name”.*
* *Consider that the SSAD should allow for standardized submission of these requested elements (including any supporting documentation)*

1. *(Purposes[[4]](#footnote-4))*

*Staff support team comment:*

*Based on EPDP Team’s categorization of use cases – will need to be reviewed. For example, for e, if RNH has provided consent there may not be a need to go through SSD? How is the data controller to know whether the consent obtained was sufficiently ‘enlightened and informed” ? What about withdrawal of consent? Once again, determination of who the relevant data controller is very important here….If I were the entity running the mechanism, I would not want to take consent on blind faith….removal of consent can be a difficult process, often misfiring, and a data controller does not want to take on the liability for another party’s sloppy management .*

*EPDP Team noted that rec 1, purpose 2 was a placeholder and should be further reviewed in the context of phase 2 deliberations. Also consider the European Commission on this topic, in its 17 April 2019 letter submitted during the public comment period and the clarifying letter sent to ICANN org on 3 May 2019.*

The EPDP Team recommends that requestors must be able to identify at a minimum from the following legitimate interests to request disclosure / access:

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

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

I think this section needs a lot of work, which I think is acknowledged here.. If we are devising the policy for disclosure, then part of the implementation of that policy would in all likelihood include guidance documents and templates for requests for data. It is difficult to avoid the conflation of the interests and the precise justification for discslosure, but it must be done, and the template must assist in this regard. Disambiguating who you are and why you want this particular registrant’s data is an imperative.

If ICANN has a purpose for release of the data, then it must be as controller of the SSAD, correct? ( is that acronym short for So Sad, by the way?) I am curious as to how the CPs are going to justify releasing all their data to ICANN to operate this thing, in many ways the CPs are still co-controllers in that case because they have delegated ICANN to do that extremely important aspect of data protection, release the third parties. Expedited release to third parties does not strike me as a valid purpose for data collection, have you run this by the DPAs and or the lawyers?

*Comments / concerns / questions to be considered in relation to building block b):*

* *Consider that legitimate interests cannot be based on the requestor but instead are based on the individual request. Consider replacing with the following instead: “The EPDP Team recommends that all requests must be sufficiently established , to the satisfaction of the controller, on a case by case basis, as having a valid legal basis”.*
* *Need to clarify the underlying rationale for providing requestors with categories of legitimate interests from which to pick. Requestors should determine their own legitimate interests, and be allowed to submit them in their own words.*
* *Further consideration of the question of accreditation may clarify this issue. The enumerated list in Building Block b) will be required in order to implement an SSAD using existing web service technologies (e.g RDAP and the technologies suggested by the TSG).*
* *Consider referring to lawful basis instead of legitimate interest - Legitimate interest is one of several possible lawful bases for disclosure of personal data.*
* *Rec 1, purpose 2: If this is an ICANN purpose, why should EPDP Team consider this further? It presupposes that ICANN is the controller. Need to avoid conflating 3rd party purposes with ICANN’s – disclosure does not need to be linked to ICANN’s purposes but upon the establishment of a legitimate interest by the 3rd party.*

1. *(User Groups[[5]](#footnote-5))*

*Staff support team comment: Based on users identified in use cases. This list will require further review and consolidation by EPDP Team.*

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

1. Criminal Law enforcement/national or public security
2. Network operator
3. Provider of online services
4. Commercial security service
5. Non-LE investigator
6. Internet user
7. Consumer protection organization
8. Social Media Companies
9. Messaging Services
10. Search Engines
11. UDRP / URS Provider
12. Copyright owners, exclusive licensees, their attorneys or agents
13. Certificate authority
14. Registered name holder (data subject)
15. Company interested in acquiring new domain name(s)
16. Operational security practitioner
17. Anti-abuse authority
18. 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. Any individual on earth can have a valid reason to request data. These may be our favorite stakeholders at ICANN, but Individuals needs to be up there as item a), not relegated to z) other

*Comments / concerns / questions to be considered in relation to building block c):*

* *Is it up to the EPDP Team to define user groups or is this addressed through accreditation? Or should groups establish their accreditation, and the SSAD must have a process for 'accepting' or verifying such accreditation? In this instance, and at its most basic, all that SSAD would be verifying is 'identity'. yup*
* *Missing from the current list “Trademarks and URS/UDRP participants”, recognizing that the overall list needs further review if it is agreed that user groups should be defined as part of this building block.*
* *Consider adding a disclosure of these specific interests to the registrant as part of the policy recommendation. All this does is help identify the parameters of what goes in the request form*

1. *(Acceptable Use Policy[[6]](#footnote-6))*

*Staff support team comment: d) From use case template: EPDP Team to further define / clarify who and how auditing is expected to be carried out.*

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

1. Must only request data from the current RDS data set (no data about the domain name registration’s history);
2. 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);
3. Must only use the data for the purpose requested;
4. Must handle the data subject’s personal data in compliance with data protection laws such as GDPR; need specific guidance here
5. Must provide representations about use of requested data which will be subject to auditing; proof of compliance with the ICANN privacy policy is what we are talking about here…or binding corporate rules
6. [Other]

[Additional requirements in the case of the following purpose [state purpose] are:

TBC based on review of use cases]

*Comments / concerns / questions to be considered in relation to building block d):*

* *Re. b), consider including reference to RAA definition of bulk access (Section 3.3.6).*
* *Re. c), further specificity would need to be provided. Consider that GDPR Art 42/43 Certification and the flipside of De-accreditation and Decertification as a mechanism to ensure the fidelity of safeguards.*
* *Re. c), consider updating as follows and striking e) (“"Must represent that requestor will only use the data for the purpose requested").*
* *Re. d), is this necessary as compliance with the law is a given?*
* *Re. d), Consider changing “such as GDPR” to “including the GDPR”.*

1. *(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. See above on compliance with privacy policy

*Comments / concerns / questions to be considered in relation to building block e):*

* *How would this be enforced? Could accreditation be used to track and enforce?*
* *Consider changing “such as GDPR” to “including the GDPR”.*
* *Once again, are we coming up with a global policy here? If so, we specify according to best practice and make the requestors sign that they will follow the policy. This may include regular audit, in the case of big requestors who want to be accredited.*

1. *(Authentication / authorization / accreditation[[7]](#footnote-7))*

*Staff support team comment:*

*Also need to address charter question a7) How can RDAP, that is technically capable, allow Registries/Registrars to accept accreditation tokens and purpose for the query? Once accreditation models are developed by the appropriate accreditors and approved by the relevant legal authorities, how can we ensure that RDAP is technically capable and is ready to accept, log and respond to the accredited requestor’s token? EPDP Team to consider reviewing Sections 5 and 6 in*[*TSG01*](https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf)*, which discusses technical requirements for credentials in RDAP.*

*Further details would need to be provided about what the benefits of accreditation are.*

*Re. “EDPB for review” - Need to confirm what happens after this review – is it ICANN Org who then modifies the implementation of the policy to add the accreditation mechanism and related requirements?*

*Re. “revocation” - Need further details on what revocation would mean in practice e.g. no further access to SSAD?*

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:

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

Those wanting to be accredited must:

1. Agree to only use the data for the legitimate and lawful purpose described above;
2. If applicable, only issue disclosure requests with respect to the trademark(s) where ownership is evidenced;
3. 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.

*Comments / concerns / questions to be considered in relation to building block f):*

* *Is accreditation necessary? Too much to write here. We continue to talk at cross purposes about accreditation. It serves no purpose other than verification of identity, unless you go for full certification or binding corporate rules in my opinion. If third parties are seeking this in order to automate access (with only self-attestation), then I think we need to ask a lot of hard questions about who is taking on the liability for these “certified” bodies.*
* *Consider equating "Accreditation" Certification under art 42/43 of the GDPR. Is there any other form of 'accreditation' that could provide anything other than verification of identity? Accreditation may be an additional layer on top of certification, specifically aimed at disclosure requests in the SSAD: it would be up to the SSAD provide to undergo a meaningful assessment of that accreditation/certification before it is deemed acceptable. If this is approach is followed, another building block would need to be added: "review and acceptance of 'accreditation' standards”.*
* *Consider whether this is the beginning of a list of enforcement considerations should or in addition to GDPR compliance (where applicable) basic entry requirements for a 3rd part accreditation to be deemed as an acceptable certification for SSAD purposes? In the latter case it would not be a requirement for "those wanting to be accredited" but a requirement on the "accrediting entity" to demonstrate and prove how they can enforce this.*
* *Consider that revocation would not be a responsibility of SSAD but of the ‘accreditation body' but the SSAD must have a way of ensuring that such a body is auditing / and enforcing requirements. Limiting or removing accreditation is the ONLY mechanism to enforce the data protection requirements of the SSAD but consider adding further details on who / how this would happen and be verified. What does this do for registrant rights? Need to consider who handles complaints, liability, and responsibility to make the registrants whole in the event of breach or malfeasance of any kind.*
* *Re. bullet 4, clarify why this is required or consider deleting it.*

**SUPPLY SIDE – Entity Disclosing The Data**

(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?)

*Comments / concerns / questions to be considered in relation to open questions:*

* *Consider whether EPDP Team should actually be referring to indemnity? At its simplest, if a contracted party gets fined, the fine/damage would be passed to someone else or shared. However, consider that this would normally be negotiated in contractual negotiations, but if it is necessary here, does it mean the policy is wrong? Or is this just an assurance that in case the EPDP Team did get it wrong, there is a backstop? Presumably ICANN lwegal has been asking Ruth these questions for their own protection. Lets get a look at that advice. The EPDP should not be developing policy in the absence of the pertinent legal advice.*

1. *(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. NO!!! where did this come from? DPAs are not there to enforce release of personal data. That is why third parties have lawyers and civil court remedies.

*Comments / concerns / questions to be considered in relation to building block g):*

* *Consider removing the reference to phase 1*
* *Consider further what role, if any, ICANN Compliance has in reviewing or assessing the substance of our legal determinations regarding disclosure. Compliance could potentially have a role in cases of non-response but legal determinations are the sole responsibility of a DPA.*
* *Consider what is the data subjects' means of redress if they feel that their data is requested wrongfully? That is a no brainer….they can complain to the DPA or a civil society group to take their case to Court.*
* *Consider whether "AND" should be an "OR" instead. The request could potentially be consistent with the policy while still violating applicable law, or vice versa, especially since there could be changes in relevant data privacy law resulting in conflict with the policy being created here.*
* *Consider "and communicate this information to the requestor" - This may not be appropriate in all circumstances; it should be further considered and possibly included as optional instead of mandatory. Guidance required on this point, local laws differ wwidely and the threshold for non-disclosure to individuals and paramountcy of law differs . (in criminal law)*
* *Also consider SLAs for requests.*

1. *(Acceptable Use Policy[[8]](#footnote-8))*

*Staff support team comment:*

Re. d), Must all requests be logged? Yes What information must be logged? There must be guidance notes on this ouot there, at a minimum, date, id of requestor, copy of template, identity of person authorized to release data, whether or not individual is entitled to notice of disclosure and if not why not. Who would be able to access the logs? This also should be logged, access limitation applies. Certainly not third parties. EPDP Team may want to consider the guidance the European Data Protection Board provided on this issue in its 5 July 2018 letter. (“The EDPB considers that, unless there is an explicit prohibition in national law, appropriate logging mechanisms should be in place to log any access to nonpublic personal data processed in the context of WHOIS. In this context, such logging is considered required as part of the security obligation of controllers (article 32), as well as the obligation and in order to be able to demonstrate compliance with the GDPR (accountability) (article 5(2))… It is up to ICANN and other controllers participating in the WHOIS system to ensure that logging information is not disclosed to unauthorized entities, in particular with a view of not jeopardizing legitimate law enforcement activities.”)

Re. e), Does this imply that the data subject is informed every time a balancing test is carried out with respect to his/her data? Not in my view….local law applies re law enforcement einvestigations. Highest standard for due process should be the basis of the policy, exceptions can be argued by the relevant third parties who request access and data controller must be permitted to refuse a fundamental violation of human rights. E.g. persecution of religious or political believers

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

1. Must only supply the necessary data requested by the requestor;
2. Must return current data in response to a request;
3. Must process data in compliance with applicable law, especially data protection laws such as GDPR and fundamental rights or constitutional protections;
4. Must log requests;
5. 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;
6. 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;
7. 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.

*Comments / concerns / questions to be considered in relation to building block h):*

* *Can this topic be addressed without confirming who the entity/entities disclosing the data is? Yes, see current work of the PETS forum and esp. Dr Ian Goldberg Uni Waterloo (Canada)*
* *How can these requirements be enforced?*
* *Re. e), consider that yes, data subjects should be informed, with the exception of sensitive LEA investigations. Consider generalizing this section as in its current form it may be too GDPR centric. This should be in the template, if law enforcement have grounds to hide their requests (and in the case of some investigation, the very act of requesting, see Goldberg anonymous queries) they must justify it to some entity, under relevant local law. Complex organized crime investigations would come in this category, need a trusted entity to authorize anonymous search capability*
* *Consider adding h) “h) Must provide [non personal] non-public data for data subjects that are legal persons or otherwise not subject to data protection laws.” Disagree strongly. Some entities are entitled to protection under constitutional law.*
* *Consider having the policy acknowledge that the SSAD be built to accommodate accredited groups, and that there should be a framework for recognizing groups that are accredited. The EDPB could then review this overall concept but may not need to have a role to review each accredited group? What is this about, different rules for different folks? Where would occasional requestors fit in this scenario? Would the save the turtles foundation be permitted to inquire about a domain name holder of the buyyourexoticturtleshere.com, or do they have to wait till their overstretched regulators bust these guys?*

1. *(Query Policy)*

*Staff support team comment:*

*Re. of an abuse nature: From use case template, consider including specific examples of what is considered abusive to ensure that no legitimate and/or authenticated requestors are blocked.*

*Rec b) From use case template: To be reworded (Marc A. and Brian to work on suggested alternative language).*

The EPDP Team recommends that the entity disclosing the data:

1. 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;
2. Must monitor the system and take appropriate action, such as revoking or limiting accThis seems to assume that we are granting access….the process imagined resembles the former WHOIS. Such voluminous requests would simply fall to the back of the line, or right off the system if not properly framed.ess, to protect against abuse or misuse of the system, such as unjustified, high-volume automated queries;
3. [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.

*Comments / concerns / questions to be considered in relation to building block i):*

* *Consider discussing this section further after the entity disclosing the data is identified.*
* *Consider any person who has breached the terms of service should be denied and prevented from being receipt of any disclosure.*
* *Re. b), how could this be enforced? Consider simplifying and merging a) and b).*
* *Re. second paragraph, consider that response should only include elements requested. Also consider further whether the response shouldn’t, must not, could, should, or must include public data elements. Consider whether reference to non-public should be removed.*
* *Check whether there is a potential conflict with policy principle #11.*
* *Consider adding: “"Each such request should be examined (either manually or programmatically) on its own merits."*
* *Consider whether query policy should include the ability to submit multiple requests if linked to the purpose cited.*

1. *(Authentication / authorization / accreditation[[9]](#footnote-9))*

*Staff support team comment:*

*Also needs to address charter question a7) How can RDAP, that is technically capable, allow Registries/Registrars to accept accreditation tokens and purpose for the query? Once accreditation models are developed by the appropriate accreditors and approved by the relevant legal authorities, how can we ensure that RDAP is technically capable and is ready to accept, log and respond to the accredited requestor’s token?*

*“re. Accreditation authority – needs a definition / description.*

The EPDP Team recommends that the entity disclosing the data must:

1. Provide the ability for confirmed accreditors to confirm accredited requestors in SSAD;
2. Provide for a mechanism to report abuse by an accredited user which is relayed to the accreditation authority for handling;
3. Confirm the validity of each request;
4. [Other]

*Comments / concerns / questions to be considered in relation to building block j):*

* *Consider addressing issue of accreditation first.*
* *Re. a), consider clarifying further.*
* *Re. b) is there a conflict of interest in having these reports relayed to the accreditation authority? How can independent review be assured?*
* *Re. c) what is meant with ‘validity’? Is this word too loaded? Does it mean to validate the credential issued to the requestor by the Accreditation body?Unless I missed something, we are not anywhere near ready to discuss these things when we don’t know what we mean by accreditation….*

**System for Standardized Access / Disclosure (SSAD)**

1. *(Receipt of acknowledgement)*

*Staff support team comment: Note, this has not been specifically discussed but is based on the EPDP Team’s recommendations developed in phase 1 of its work. Will need to be cross-checked with implementation of phase 1 recommendations.*

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. I hope this includes an opportunity for the individual to object…

*Comments / concerns / questions to be considered in relation to building block k):*

* *Dependent on what SSAD actually is. Is the SSAD a centralized concept or just a decentralized concept that contracted parties implement?*
* *Consider that if implementation of any SSAD using modern web service technologies and frameworks acknowledgement of the receipt of the request MUST be instantaneous.*

1. *(Query Policy)*

The EPDP Team recommends the SSAD, in whatever form it eventually takes, MUST:

1. Unless otherwise required or permitted, not allow bulk access,[[10]](#footnote-10) wildcard requests, reverse lookups, nor boolean search capabilities.
2. Must only return current data (no data about the domain name registration’s history);
3. Must receive a specific request for every individual domain name (no bulk access[[11]](#footnote-11));
4. 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).

*Comments / concerns / questions to be considered in relation to building block l):*

* *Dependent on decision on what SSAD actually is.*
* *Further consider bulk access, wildcard requests, reverse lookups or boolean search capabilities – should these not be allowed in any circumstance, or should these be allowed to accommodate some of the use cases identified? LEAs have different rights*

1. *(Terms of use / disclosure agreements / privacy policies)*

The EPDP Team recommends that [TBC]

1. *(Financial sustainability)*

The EPDP Team recommends that [TBC]

*Comments / concerns / questions to be considered in relation to building block n):*

* *Consider when to consider this question in further detail, in the early stages or after a number of fundamental questions have been answered?*
* *All considerations of demand, expectations, likely outgoings, funding, sustainability, staffing, enforcement, cost benefits analysis etc. should be considered by the EPDP Team and approached from a realistic point of view.*
* *Consider whether commercial entities should pay for access/disclosure and ensure a link between cost recovery and cost causation. Please keep in mind that in some jurisdictions, individuals have to pay for access to their own data under DP law. It is deeply offensive t think of downloading these costs on the registrant, via the CPS. Of course requestors should pay.*
* *Consider insurance options as ways of mitigating risk and accreditation fees. Put the rights of the individual first here….no amount of insurance will get back person data once it is gone. WE are not here to mitigate data controllers’ risks at the expense of the registrants (by providing additional insurance costs in the system that ultimately individuals will pay…and the higher the risk the higher the premiums. Lets make an effort to do this right.*

**SSAD IMPLEMENTATION GUIDANCE**

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.

*Comments / concerns / questions to be considered in relation to implementation guidance #i):*

* *Further consideration should be given to this guidance point; it could be used to circumvent the 'no bulk access' requirement.*

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

*Comments / concerns / questions to be considered in relation to implementation guidance #ii):*

* *Consider whether there is a conflict with policy principle #11? Why is it necessary to also provide publicly-available registration data? Cost issues are key here. If it is easy enough to link the public data, this should not be a problem , and may also serve to help make sure accurate requests/disclosures are made. Separating the data always risks error, does it not?.*

1. Charter question a2 [↑](#footnote-ref-1)
2. Charter question a3 [↑](#footnote-ref-2)
3. Charter question a5 and a6 [↑](#footnote-ref-3)
4. Charter question a1 [↑](#footnote-ref-4)
5. Charter question a4 [↑](#footnote-ref-5)
6. Charter questions c1-7 [↑](#footnote-ref-6)
7. Charter questions b1, b2 and b3 [↑](#footnote-ref-7)
8. Charter questions c1-7 [↑](#footnote-ref-8)
9. Charter questions b1, b2 and b3 [↑](#footnote-ref-9)
10. As described in section 3.3.6 of the Registrar Accreditation Agreement [↑](#footnote-ref-10)
11. As defined in section 3.3.6 of the Registrar Accreditation Agreement. [↑](#footnote-ref-11)