EPDP TEAM WORKSHEET

Topic	Last updated	Priority
System for Standardized Access/Disclosure to Non-Public Registration Data (SSAD)	27 May 2019	1

ISSUE DESCRIPTION AND/OR CHARTER QUESTIONS

From the EPDP Team Charter:

(a) Purposes for Accessing Data – What are the unanswered policy questions that will guide implementation?

a1) Under applicable law, what are legitimate purposes for third parties to access registration data?
a2) What legal bases exist to support this access?
a3) What are the eligibility criteria for access to non-public Registration data?
a4) Do those parties/groups consist of different types of third-party requestors?
a5) What data elements should each user/party have access to based on their purposes?
a6) To what extent can we determine a set of data elements and potential scope (volume) for specific third parties and/or purposes?
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?

(b) Credentialing – What are the unanswered policy questions that will guide implementation?

b1) How will credentials be granted and managed?
b2) Who is responsible for providing credentials?
b3) How will these credentials be integrated into registrars'/registries' technical systems?

(c) Terms of access and compliance with terms of use – What are the unanswered policy questions that will guide implementation?

Commented [1]: The GAC Small Group thinks this is an excellent tool for informing and tracking progress on this priority issue. We expect that this document will continue to evolve as our work gets underway.

Commented [2]: We should replace "access" by "be granted disclosure" or similar throughout the document. Access should only refer to access of the data subject to their own data and supplemental data linked to it.

Commented [3]: Since data may be transmitted to 3rd parties under a variety of bases, including consent, we could flip this around. Rather than "for third parties to <choose a verb here> registration data", replace with "for transmission of registration data to third parties"

Commented [4]: I don't know, Volker. IPC doesn't care what we call the "SSAD" but "granting disclosure" sounds like there should be a 6.1(f) test. We need to work on standardized (standardized=consistent across CPs) access. This needs to relieve CPs of doing the "granting," in favor of sufficient legal protections that allow lawful access.

Commented [5]: I don't understand what you mean by relieving CPs of doing the granting. who would grant it then? The parties just access it on their own with no granting?

Commented [6]: i'm sorry Brian, can you clarify what you are saying here? To be clear, for EVERY party outside of public authorities, or those empowered by law to have data disclosed to them, requests for disclosure, even in the SSAD, will always be 6(1)f and the will always attract the balancing test.

If you are referring to Law Enforcement (and other so empowered public authorities), should they even want to use the SSAD, must rely on 6(1)e , 6(1)c and ... [1]

Commented [7]: Mark S, I'm sorry can you clarify also.. what other legal basis? You note consent! I'm struggling with this , unless you are thinking that we get that consent on a case by case basis, upon receipt ... [2]

Commented [8]: There are two separate issues in your response. If an Office 365 subscriber tells us to view their registration data in order to verify that they own the domain name that they bring to their subscription ... [3]

Commented [9]: Mark, that is consent you have obtained, as a Data Controller (and indeed as a company providing service that you have deemed to require an element of such confirmation) in a separate ... [4]

Commented [10]: There will have to be granting, either by the CPs or by an entity the CPs outsource the granting to. The standardization is supposed to get rid of differences between CPS as much as possible, but ... [5]

Commented [11]: I thought we'd defined Registration Data in the Phase 1 Final Report. If so, suggest we capitalize here (and throughout) to clarify that we're intending to refer to the defined term.

Commented [12]: One important issue that we need to discuss is whether we need an accreditation model.

c1) What rules/policies will govern users' access to the data?
c2) What rules/policies will govern users' use of the data once accessed?
c3) Who will be responsible for establishing and enforcing these rules/policies?
c4) What, if any, sanctions or penalties will a user face for abusing the data, including future restrictions on access or compensation to data subjects whose data has been abused in addition to any sanctions already provided in applicable law?
c5) What kinds of insights will Contracted Parties have into what data is accessed and how it is used?
c6) What rights do data subjects have in ascertaining when and how their data is accessed and used?
c7) How can a third party access model accommodate differing requirements for data subject notification of data disclosure?

From the Annex to the Temporary Specification:

- Developing methods to provide potential URS and UDRP complainants with sufficient access to Registration Data to support good-faith filings of complaints
- Limitations in terms of query volume envisaged under an accreditation program balanced against realistic investigatory cross-referencing needs.
- Confidentiality of queries for Registration Data by law enforcement authorities
- Pursuant to Section 4.4, continuing community work to develop an accreditation and access model that complies with GDPR, while recognizing the need to obtain additional guidance from Article 29 Working Party/European Data Protection Board.
- Consistent process for continued access to Registration Data, including non-public data, for users with a legitimate purpose, until the time when a final accreditation and access mechanism is fully operational, on a mandatory basis for all contracted parties.

From EPDP Team Phase 1 Final Report:

EPDP Team Recommendation #3.
In accordance with the EPDP Team Charter and in line with Purpose #2, the EPDP Team undertakes to make a recommendation pertaining to a standardised model for lawful disclosure of non-public Registration Data (referred to in the Charter as 'Standardised Access') now that the gating questions in the charter have been answered. This will include addressing questions such as:

- Whether such a system should be adopted
- What are the legitimate purposes for third parties to access registration data?
- What are the eligibility criteria for access to non-public Registration data?
- Do those parties/groups consist of different types of third-party requestors?
- What data elements should each user/party have access to?

In this context, the EPDP team will consider amongst other issues, disclosure in the course of intellectual property infringement and DNS abuse cases. There is a need to confirm that

Commented [13]: Lesser involvement by CPs here will lessen CP liability.

Commented [14]: Actually the opposite is true. Lesser involvement by the CPs (depending on who is presenting the data for the SSAD database) means that they will likely have larger incentive (and liability) to ensure it is being conducted properly. This is not as simple as passing the Data hot potato.

Commented [15]: GDPR requires clarity. Must build exception mechanism for LEA investigations that should not be visible to registrant.

Commented [16]: I think the PSWG says this in a much more nuanced way and well in a less scary way. not all LEAs are legitimate.

Commented [17]: See SSAC 101 on negative effects of rate-limiting.

Commented [18]: If any group thinks the answer to this might be "no," we need to know and address this immediately. Otherwise, we need to agree "yes" (per the charter) and move on to "how."

Commented [19]: So this question might have been addressing a centralized accreditation, access mechanism. and I agree the order has to be changed. But I think some the questions in the final report might actually relate to the questions in the charter.(for example the purpose question)

Commented [20]: Perhaps we should a tad more contemplative in our approach. This is not about whether we want it or not, it's about legality. Is your answer of "yes" based on the fact that you would like system, or whether, upon careful consideration of the facts, and legal nuances, that we SHOULD adopt it. We can only answer this when we establish the base line answers to key legal questions. I appreciate the enthusiasm, but let's complete the processes first.

disclosure for legitimate purposes is not incompatible with the purposes for which such data has been collected.

TSG Policy Questions

1. Result from the EPDP, or other policy initiatives, regarding access to non-public gTLD domain name registration data.
2. Identify and select Identity Providers (if that choice is made) that can grant credentials for use in the system.
3. Describe the general qualifications of a Requestor that is authorized to access non-public gTLD domain name registration data, such as which sorts of Requestors get access to which fields of non-public gTLD domain name registration data ("the authorization policy").
4. Detail whether a particular category of Requestors or Requestors in general, can download logs of their activity.
5. Describe data retention requirements imposed on each component of the system.
6. Describe service Level Requirements (SLRs) for each component of the system, including whether those SLRs and evaluations of component operators against them are made public, and for handling complaints about access.
7. Specify legitimate causes for denying a request.
8. Outline support for correlation via a pseudonymity query as described in Section 7.2.
9. Outline the selection of an actor model as described in Section 8 and the appropriate supported components and service discovery as described in Sections 10.1 through 10.5.
10. Describe the conditions, if any, under which requests would be disclosed to CPs.
11. Provide legal analysis regarding liability of the operators of various components of the system.
12. Outline a procedure for fielding complaints about inappropriate disclosures and, accordingly, an Acceptable Use Policy.

EXPECTED DELIVERABLE

Policy recommendations for a standardised model for lawful disclosure/access of non-public Registration Data

GENERAL REQUIRED READING

Commented [21]: The GAC recognizes that this text comes directly from the TSG report, but wanted to flag that it is our view that this item is outside the scope of the EPDP.

Commented [22]: Agreed. We do not need to identify the providers, just set the basic standards that such providers would have to meet. The rest is for the IRT to decide.

Commented [23]: This seems to be a backwards approach. Before we even get to reasons for denial, we need to define requirements for making a legitimate request in the first place.

Commented [24]: I think IPC agrees with Volker here. In fact, we're in a better legal position if we focus on establishing parameters within which an access demand will always be legal for the fulfilling party to fulfill.

Commented [25]: Again a backwards question that should rather refer to the conditions under which a requests would NOT be disclosed to CPs. The very act of disclosure of non-public data by CPs in and of itself requires disclosure of the request to CPs. How else should requests be evaluated by the legally liable parties?

Commented [26]: I think IPC agrees with Volker here too. And we should not assume that the CPs will be the party "doing the disclosing," "providing the access," "transmitting the data," etc. If the CP is not involved in this, it would be inappropriate for the CP to know about the data disclosure/access/transmission.

Commented [27]: This is important. It's called "safeguards" in GDPR parlance.

Commented [28]: I don't think this is a material change, but I feel it's more accurate to say the expected output is "Policy recommendations..."

Deleted: A

Commented [29]: +1

Description	Link	Required because
Framework Elements for Unified Access Model for Continued Access to Full WHOIS Data (18 June 2018)	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-18jun18-en.pdf	
Draft Accreditation and Access model for non-public WHOIS DATA (BC/IPC)	Model Version 1.7 dated 23 July 2018	
The Palage Differentiated Registrant Data Access Model (aka Philly Special)	The Palage Differentiated Registrant Data Access Model (aka Philly Special) - Version 2.0 dated 30 May 2018	
Unified Access Model for Continued Access to Full WHOIS Data - Comparison of Models Submitted by the Community (18 June 2018)	https://www.icann.org/en/system/files/files/draft-unified-access-model-summary-elements-18jun18-en.pdf	
Article 29 WP Opinion 2/2003 on the application of the data protection principles to the Whois directories (2003)	https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp76_en.pdf	
EWG Report Section 4c, RDS User Accreditation Principles (June 2014)	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf	

EWG Research – RDS User Accreditation RFI	https://community.icann.org/download/attachments/45744698/EWG%20USER%20ACCREDITATION%20RFI%20SUMMARY%2013%20March%202014.pdf	
Part 1: How it works: RDAP – 10 March 2019	https://64.schedule.icann.org/meetings/963337	
Part 2: Understanding RDAP and the Role it can Play in RDDS Policy - 13 March 2019	https://64.schedule.icann.org/meetings/961941	
Technical Study Group on Access to Non-Public Registration Data Proposed Technical Model for Access to Non-Public Registration Data (30 April 2019)	TSG01, Technical Model for Access to Non-Public Registration Data	
Final Report on the Privacy & Proxy Services Accreditation Issues (7 December 2015) ● Definitions - pages 6-8 ● Annex B – Illustrative Disclosure Framework applicable to Intellectual Property Rights-holder Disclosure Requests – pages 85 – 93 ● Draft Privacy & Proxy Service Provider Accreditation Agreement	https://gnso.icann.org/sites/default/files/filefield_48305/ppsai-final-07dec15-en.pdf	

BRIEFINGS TO BE PROVIDED

Topic	Possible presenters	Important because
RDAP – Q & A session post review of ICANN 65 sessions	Francisco Arias, ICANN Org	Ensure a common understanding of the workings and abilities of RDAP

DEPENDENCIES

Describe dependency	Dependent on	Expected or recommended timing
The negotiation and finalization of the data protection agreements required according to phase 1 report are a prerequisite for much of work in phase 2 (suggested by ISPCP)	CPs/ICANN Org	

PROPOSED TIMING AND APPROACH

Introduction

Objective of EPDP Team is to develop and agree on rules and requirements for sharing of non-public registration data with requesting parties (System for Standardized Access/Disclosure of Non-Public Registration Data).

Until legal assurances satisfactory to the contracted parties are provided, the development of the policy recommendations for a System for Standardized Disclosure/Access will be agnostic to the modalities of the System.

In parallel, the EPDP Team as a whole should engage with ICANN Org on the development of policy questions that will help inform the discussions with DPAs which have as its objective to determine what model of System for Standardized Disclosure would be fully compliant with GDPR, workable and address/alleviate the legal liability of contracted parties.

Non-exhaustive list of topics expected to be addressed:

Commented [30]: From IPC: The "Introduction" text on page 6 should specify our objective is to agree to recommendations and policy related to the sharing of non-public registration data, not "rules and requirements".

Commented [31]: I would suggest using "policy recommendations" here.

Commented [32]: See my previous comment about Registration Data as a defined term.

Commented [33]: The GAC is not wedded to the term "requesting" here, but cautions limiting this model to "third" parties in the strictest sense of the meaning. Specifically, we need to also consider whether and how ICANN and its contracted parties fit in this.

Deleted: third

Commented [34]: As noted previously, the GAC is of the view that legal "assurances" is the best placed term here as legal "certainty" is rarely ascertainable in the business world.

Commented [35]: Suggest to replace "contracted" with "relevant" or similar. IPC expects that users of the system, who will be data processors under GDPR, will also have legal concerns which will require assurances.

Commented [36]: Added to clarify that the legal assurances should be satisfactory the contracted parties. Legal assurances provided to ICANN, esp. by its own counsel, may not provide the requisite level of assurance to contracted parties.

Deleted: certainty is

- Terminology and Working Definitions
- Legal guidance needed
- Requirements, incl. defining user groups, criteria & format of request
- Publication of process, format and content request required
- Timeline of process
- Receipt of acknowledgment
- Accreditation
- Authentication
- Purposes for third party disclosure
- Lawful basis for disclosure
- Code of conduct
- Terms of use / disclosure agreements
- Privacy policies
- Query volume limitations
- Retention and destruction of data
- Service level agreements
- Financial sustainability

Approach

Determine at the outset:

a) Terminology and working definitions
b) Identify legal guidance needed (note, this is also an ongoing activity throughout all the topics).

Possible logical order to address the remaining topics:

c) Define user groups, criteria and purposes / lawful basis per user group
↓
d) authentication / accreditation of user groups
↓
e) format of requests per user group
↓
f) query limitations
↓
g) receipt of acknowledgement, including timeline
↓
h) response requirements / expectations, including timeline/SLAs
↓
i) code of conduct
↓

Commented [37]: From IPC: The third bullet suggests we will be deciding the "Format" of request. The EPDP should not be concerning itself with issues of "format". We need to focus on setting policy around the criteria and "contents" of requests, including which data/fields are mandatory and which may be optional.

Commented [38]: From IPC: The fourth bullet also mentions format - as above we should focus on the "what" not the "how".

Commented [39]: From IPC: Add: Authorization (its a result of the accreditation) along with Authentication (identification).

Commented [40]: expand to "lawful basis and fulfillment of legal requirements" to also include considerations of cross-border transfers of data that requester may need to meet.

Commented [41]: I think this concept better fits into "Terms of use / disclosure agreements"

Commented [42]: Agreed with Mark. To Volker's point, let's do better and build in contractual safeguards that eliminate cross-border issues.

Commented [43]: From IPC: We believe that we should not pre-suppose or assume the use of a code of conduct at this point in time. There may be other options available to us that will allow us to achieve the same goal.

Commented [44]: "code of conduct" has a different, specific meaning under GDPR. Here, we actually mean "acceptable use policy"

Commented [45]: From IPC: As stated above we should not pre-suppose or assume the use of a code of conduct at this point in time. Perhaps a more generic term should be used. Also things like terms of use/disclosure agreements/SLAs/data retention and discussion may be included in a CoC/Contract so perhaps we can merge these into a single bullet.

Commented [46]: From IPC: We believe the order OK. See above regarding the use of a more generic term for Code of Conduct.

j) terms of use / disclosure agreements / privacy policies

↓

k) retention and destruction of data

l) Overall topic of consideration: financial sustainability

Hereunder further details for each of these topics has been provided. To jump to each section, please use the links below:

Following the completion of this effort, each topic (including Phase 1 topics) and its scope of work will form the basis of an overall scheduled work plan. Some topics may be addressed in parallel, while others may have dependencies to other work before more informed deliberations can be had. Each topic will be given a set time to conduct issue deliberations, formulate possible conclusions and or possible recommendations to the policy questions. Conclusions or recommendations that obtain a general level of support will advance forward for further consideration and refinement towards an Initial Report. The goal is to achieve levels of consensus on the proposal(s) where possible prior to publication.

Commented [47]: From IPC: Based on my question on the last call, let's clarify the text at the end of page 8. Replace "Following the completion of this effort" with "After receiving input from the EPDP team on this Worksheet, each topic…."

Commented [48]: From IPC: To avoid confusion or misinterpretation we should avoid paraphrasing or summarizing Phase 1 recommendation language.

a) Topic: Terminology and Working Definitions

Objective: To ensure that the same meaning is associated with the terms used in the context of this discussion and avoid confusion, the EPDP Team is to agree on a set of working definitions. It is understood that these working definitions merely serve to clarify terminology used, it is in no way intended to restrict the scope of work or predetermine the outcome. It is understood that these working definitions will need to be reviewed and revised, as needed, at the end of the process.

Materials to review:

- Terminology used in GDPR and other data protection legislation
- Final Report on the Privacy & Proxy Services Accreditation Issues (7 December 2015) - eDefinitions - pages 6-8

Related mind map question: None

Related EPDP Phase 1 Implementation: To be confirmed - recommendation #18 implementation may include definitions that may need to be factored into the EPDP Team's phase 2 deliberations.

Tasks:

- Confirm whether any definitions are expected to be developed or applied in the implementation of recommendation #18 (Staff)
- Develop first draft of working definitions. (Staff)
- EPDP Team to review and provide input (EPDP)
- Obtain agreement on base set of definitions (EPDP)
- Maintain working document of definitions through deliberations (All)

Target date for completion: 30 May 2019

b) Topic: Legal Questions

Objective: identify legal questions that are essential to help inform the EPDP Team deliberations on this topic.

Questions submitted to date:

Question	Status	Owner
There is a need to confirm that disclosure for legitimate purposes is not incompatible with the purposes for which such data has been collected.	From rec #3 of the phase 1 Final Report	
Answer the controllership and legal basis question for a system for Standardized Access to Non-Public Registration Data, assuming a technical framework consistent with the TSG, and in a way that sufficiently addresses issues related to liability and risk mitigation with the goal of decreasing liability risks to Contracted Parties through the adoption of a system for Standardized Access	(Suggested by IPC)	
Legal guidance should be sought on the possibility of an accreditation-based disclosure system as such.	(Suggested by ISPCP)	
The question of disclosure to non-EU law enforcement based on Art 6 I f GDPR should be presented to legal counsel.	(Suggested by ISPCP)	
Can a centralized access/disclosure model (one in which a single entity is responsible for receiving disclosure requests, conducting the balancing test, checking accreditation, responding to requests, etc.) be designed in such a way as to limit the liability for the contracted parties to the greatest extent possible? IE - can it be opined that the centralized entity can be largely (if not entirely) responsible for the liability associated with disclosure (including the accreditation and authorization) and could	(Suggested by GAC)	

Deleted: Other?

Commented [49]: The GAC Small Group posed this question to the EPDP on May 30.

the contracted parties' liability be limited to activities strictly associated with other processing not related to disclosure, such as the collection and secure transfer of data? If so, what needs to be considered/articulated in policy to accommodate this?		

Formatted: Font color: Auto

Tasks:

- Determine priority questions for phase 2 related topics
- Agree on approach and approval process for questions that emerge throughout deliberations

Target date for completion: Ongoing

c) Topic: Define user groups, criteria and purposes / lawful basis per user group

Objective:

- Define the categories of user groups that may request disclosure of / access to non-public registration data as well as the criteria that should be applied to determine whether an individual or entity belongs to this category.
- Determine purposes and lawful basis per user group for processing data
- Determine if and how the Phase 2 standardized framework can accommodate requests unique to large footprint groups. Consider if those not fitting in any of the user groups identified may still request disclosure/access through implementation of recommendation #18 or other means.

Commented [50]: From IPC: General comment: The main objective of this exercise is to ensure we discuss and answer (in the form of recommendations) the charter questions as defined in the "System for Standardized Access to Non Public Registration Data". Answering these charter questions should be included in the "objective" for each topic (as or if applicable). We notice that the charter questions are referenced in the "Related mind map questions" section of each topic, and in many cases charter questions are referenced in multiple topics, however we believe it is in the teams best interest to discuss and answer each charter question in a single "place" with the goal of avoiding (or minimizing to the greatest extent possible) the re-opening and re-debate of decisions previously made.

Materials to review:

Description	Link	Required because
At the end of June 2017, ICANN asked contracted parties and interested stakeholders to identify user types and purposes of data elements required by ICANN policies and contracts. The individual responses received and a compilation of the responses are provided below.	Dataflow Matrix, Compilation of Responses Received – Current Version	Most recent effort to identify user types
EWG Final Report sets forth a non-exhaustive summary of users of the existing WHOIS system, including those with constructive or malicious purposes. Consistent with the EWG's mandate, all of these users were examined to identify existing and possible future workflows and the stakeholders and data involved in them.	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf - pages 20-25	
Review purposes established and legal basis identified in phase 1 of the EPDP Team	https://gnso.icann.org/en/drafts/epdp-gtld-registration-data-specs-final-20feb19-en.pdf (pages 34-36 / 67-71)	

GDPR Relevant provisions	Relevant provisions in the GDPR - See Article 6(1), Article 6(2) and Recital 40	
ICO lawful basis for processing info page	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/	

Related mind map questions:

P1-Charter-a
(a) Purposes for Accessing Data – What are the unanswered policy questions that will guide implementation?

a1) Under applicable law, what are legitimate purposes for third parties to access registration data?
a2) What legal bases exist to support this access?
a3) What are the eligibility criteria for access to non-public Registration data?
a4) Do those parties/groups consist of different types of third-party requestors?

Annex to the Temporary Specification:
3. Developing methods to provide potential URS and UDRP complainants with sufficient access to Registration Data to support good-faith filings of complaints.

Phase 1 Recommendations
EPDP Team Rec #3

- What are the legitimate purposes for third parties to access registration data?
- What are the eligibility criteria for access to non-public Registration data?
- Do those parties/groups consist of different types of third-party requestors?

The EPDP Team requests that when the EPDP Team commences its deliberations on a standardized access framework, a representative of the RPMs PDP WG shall provide an update on the current status of deliberations so that the EPDP Team may determine if/how the WG's recommendations may affect consideration of the URS and UDRP in the context of the standardized access framework deliberations.

Note that Purpose 2 is a placeholder pending further work on the issue of access in Phase 2 of this EPDP and is expected to be revisited once this Phase 2 work has been completed. [staff

note - linked to purposes but timing to revisit purpose 2 is once phase 2 work has been completed]

TSG-Final-Q#3
3. Describe the general qualifications of a Requestor that is authorized to access non-public gTLD domain name registration data, such as which sorts of Requestors get access to which fields of non-public gTLD domain name registration data ("the authorization policy").

Related EPDP Phase 1 Implementation:
None expected

Tasks:

- Develop first list of categories of requestors based on source materials. (Staff)
- Review list of categories of requestors and determine eligibility criteria. (All)
- Develop abuse types and scenarios to formulate use cases that determine requirements for each requestor
- Determine purposes and legal basis per user group for processing data (All)
- Determine if and how the Phase 2 standardized framework can accommodate requests unique to large footprint groups. Consider if those not fitting in any of the user groups identified may still request disclosure/access through implementation of recommendation #18 or other means. (All)
- Confirm all charter questions have been addressed and documented.

Target date for completion: 13 June 2019
(Revisit purpose 2 - once phase 2 work has been completed)

Commented [51]: From IPC: General comment Ensure tasks for each topic allow for, at a minimum, answering the relevant charter questions.
Can we map each charter question into a single SSAD topic, to ensure we do not miss anything and avoid any duplication of effort?

Commented [52]: From IPC: General comment We suggest once we agree with a delivery date date we work back from that date with a work plan to address all issues that need to be worked on.

d) Authentication / accreditation of user groups

Objective:

- Establish if authentication and/or accreditation of user groups should be required
  - Can an accreditation model compliment or be used with what is implemented from EPDP-Phase 1 Recommendation #18?
- If so, establish policy principles for authentication and/or accreditation, including addressing questions such as:
  - whether or not an authenticated user requesting access to non-public WHOIS data must provide its legitimate interest for each individual query/request.
- If not, explain why not and what implications this might have on queries from certain user groups, if any.

Materials to review:

Description	Link	Required because
Identification and authentication in the TSG model	https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf page 23-24	
EWG Final Report - RDS Contact Use Authorization and RDS User Accreditation Principles	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf page 39-40 and page 62-67	
Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data - How would authentication requirements for legitimate users be developed?	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-20aug18-en.pdf pages 9-10, 10-11, 18, 23	

Related mind map questions:

P1-Charter-a/b

(a) Purposes for Accessing Data - What are the unanswered policy questions that will guide implementation?

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?

(b) Credentialing – What are the unanswered policy questions that will guide implementation?
b1) How will credentials be granted and managed?
b2) Who is responsible for providing credentials?
b3) How will these credentials be integrated into registrars'/registries' technical systems?

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?

Annex to the Temporary Specification

1. Pursuant to Section 4.4, continuing community work to develop an accreditation and access model that complies with GDPR, while recognizing the need to obtain additional guidance from Article 29 Working Party/European Data Protection Board.

TSG-Final-Q#2

Identify and select Identity Providers (if that choice is made) that can grant credentials for use in the system.

Related EPDP Phase 1 Implementation:
None expected.

Tasks:

- Review materials listed above and discuss perspectives on authentication / authorization.(EPDP)
- Confirm definitions of key terms Authorization, Accreditation and Authentication
- Determine full list of policy questions and deliberate each
- Determine possible solutions or proposed recommendation, if any
- Confirm all charter questions have been addressed and documented

Target date for completion: ICANN 65

e) Format of requests per user group

Commented [53]: From IPC: References "format" again. Should focus on content of requests and responses. (what is required)

Objective: establish minimum policy requirements, criteria and format for requests per user group as identified under c.

Materials to review:

Description	Link	Required because
• Annex B – Illustrative Disclosure Framework applicable to IntellectualProperty Rights-holder Disclosure Requests – pages 85 – 93 • Privacy & Proxy Service Provider Accreditation Agreement	Final Report on the Privacy & Proxy Services Accreditation Issues (7 December 2015)	
Example: .DE Information & Request Form	https://www.denic.de/en/service/whois-service/third-party-requests-for-holder-data/ https://www.denic.de/fileadmin/public/downloads/Domaindatenanfrage/Antrag_Domaindaten_Rechteinhaber_EN.pdf	
Example: Nominet Request Form	https://s3-eu-west-1.amazonaws.com/nominet-prod/wp-content/uploads/2018/05/22101442/Data-request-form.pdf	

Related mind map questions:

P1-Charter-c
c1) What rules/policies will govern users' access to the data?

Related EPDP Phase 1 Implementation:

Recommendation #18 (but does NOT require automatic disclosure of information)

Minimum Information Required for Reasonable Requests for Lawful Disclosure:

- Identification of and information about the requestor (including, the nature/type of business entity or individual, Power of Attorney statements, where applicable and relevant);
- 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?);
- Affirmation that the request is being made in good faith;
- A list of data elements requested by the requestor and why this data is limited to the need;
- Agreement to process lawfully any data received in response to the request.

Tasks:

- Confirm implementation approach for recommendation #18
- Confirm definitions of key terms
- Determine full list of policy questions and deliberate each
- Determine possible solutions or proposed recommendation, if any
- Confirm all charter questions have been addressed and documented

Target date for completion: ICANN 65

Commented [54]: add: applicable jurisdiction(s) of requestor and anyone requestor intents to make data available to

Commented [55]: Volker: a step better might be a data processing agreement that includes sufficient contractual guarantees to make the requestor's jurisdiction irrelevant.

Commented [56]: Depends. If you have an agreement there is freedom to contract (or not to contract). It also puts the enforcement onus on the party that has suffered the terms of the agreement having been breached. Finally, a two-party agreement structure would allow bad actors to continue their abusive use with other contracted parties.

Commented [57]: Let's think big-picture on this and not individual request-by-request basis.

f) Query limitations

Commented [58]: From IPC: The header/term "query limitations" doesn't quite describe the set of objectives listed and is misleading/confusing. Perhaps "Query Policy" would be better.

Objective: Establish minimum policy requirements for logging of queries, defining the appropriate controls for when query logs should be made available, and if there should be query limitations for authenticated and unauthenticated users of the SSAD.

- How will access to non-public registration data be limited in order to minimize risks of unauthorized access and use (e.g. by enabling access on the basis of specific queries only as opposed to bulk transfers and/or other restrictions on searches or reverse directory services, including mechanisms to restrict access to fields to what is necessary to achieve the legitimate purpose in question)?
- Should confidentiality of queries be considered, for example by law enforcement?
- How should query limitations be balanced against realistic investigatory cross-referencing needs?

Materials to review:

Description	Link	Required because

Related mind map questions:

P1-Charter-a
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?

Annex to the Temporary Specification:
6 Limitations in terms of query volume envisaged under an accreditation program balanced against realistic investigatory cross-referencing needs.
7 Confidentiality of queries for Registration Data by law enforcement authorities.

Related EPDP Phase 1 Implementation: None.

Tasks:
- Confirm definitions of key terms

- Determine full list of policy questions and deliberate each
- Determine possible solutions or proposed recommendation, if any
- Confirm all charter questions have been addressed and documented

Target date for completion: ICANN 65

g) Receipt of acknowledgement, including timeline

Objective: Define policy requirements around timeline of acknowledgement of receipt and additional requirements (if any) the acknowledgement should contain.

What, if any, are the baseline minimum standardized receipt of acknowledgement requirements for registrars/registries? What about 'urgent' requests and how are these defined?

Materials to review:

Description	Link	Required because
Phase 1 Final Report Rec. 18 Timeline & Criteria for Registrar and Registry Operator Responses	https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf p. 19	

Related mind map questions:

P1-Charter-c
c1) What rules/policies will govern users' access to the data?

Related EPDP Phase 1 Implementation: - Recommendation #18*:*
Timeline & Criteria for Registrar and Registry Operator Responses -
Registrars and Registries must reasonably consider and accommodate requests for lawful disclosure:
• Response time for acknowledging receipt of a Reasonable Request for Lawful Disclosure. Without undue delay, but not more than two (2) business days from receipt, unless shown circumstances does not make this possible.

Tasks:

- Confirm definitions of key terms
- Determine full list of policy questions and deliberate each
- Determine possible solutions or proposed recommendation, if any
- Confirm all charter questions have been addressed and documented

Target date for completion: TBD

h) Response requirements / expectations, including timeline/SLAs

Objective: Define policy requirements around response requirements, including addressing questions such as:

- including addressing questions such as:
  - Whether or not full WHOIS data must be returned when an authenticated user performs a query.
  - What should be the SLA commitments for responses to requests for access/disclosure
  - What are the minimum requirements for responses to requests, including denial of requests?

Materials to review:

Description	Link	Required because
Phase 1 Final Report Rec. 18 Timeline & Criteria for Registrar and Registry Operator Responses	https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf p. 19	
Final Report on the Privacy & Proxy Services Accreditation Issues (7 December 2015) ● Annex B – Illustrative Disclosure Framework applicable to Intellectual Property Rights-holder Disclosure Requests – pages 90 - 92	https://gnso.icann.org/sites/default/files/filefield_48305/ppsai-final-07dec15-en.pdf	Section of PPSAI illustrative disclosure framework detailing required minimum response

Related mind map questions:

P1-Charter-a/c
a5) What data elements should each user/party have access to based on their purpose?
a6) To what extent can we determine a set of data elements and potential scope (volume) for specific third
parties and/or purposes?
c1) What rules/policies will govern users' access to the data?

Phase 1 Recommendation - #3

What data elements should each user/party have access to?

Annex to the Temporary Specification
2. Addressing the feasibility of requiring unique contacts to have a uniform anonymized email address across domain name registrations at a given Registrar, while ensuring security/stability and meeting the requirements of Section 2.5.1 of Appendix A.

TSG-Final-Q#6
Describe service Level Requirements (SLRs) for each component of the system, including whether those SLRs and evaluations of component operators against them are made public, and for handling complaints about access.
TSG-Final-Q#7
Specify legitimate causes for denying a request.
TSG-Final-Q#8
Outline support for correlation via a pseudonymity query as described in Section 7.2.

Related EPDP Phase 1 Implementation*:*
Recommendation #18:

- Requirements for what information responses should include. Responses where disclosure of data (in whole or in part) has been denied should include: rationale sufficient for the requestor to understand the reasons for the decision, including, for example, an analysis and explanation of how the balancing test was applied (if applicable).
- Logs of Requests, Acknowledgements and Responses should be maintained in accordance with standard business recordation practices so that they are available to be produced as needed including, but not limited to, for audit purposes by ICANN Compliance;
- Response time for a response to the requestor will occur without undue delay, but within maximum of 30 days unless there are exceptional circumstances. Such circumstances may include the overall number of requests received. The contracted parties will report the number of requests received to ICANN on a regular basis so that the reasonableness can be assessed.
- A separate timeline of [less than X business days] will considered for the response to 'Urgent' Reasonable Disclosure Requests, those Requests for which evidence is supplied to show an immediate need for disclosure [time frame to be finalized and criteria set for Urgent requests during implementation].

Tasks:

- Confirm definitions of key terms
- Determine full list of policy questions and deliberate each
- Determine possible solutions or proposed recommendation, if any
- Confirm all charter questions have been addressed and documented

Target date for completion: August

Commented [59]: may need legal review of question whether uniform anonymized data may also be considered personal data.

Commented [60]: As I mentioned on the call, that is too broad. The specific methods of pseudonymization/anonymization must be reviewed, not the overall concept of pseudo/anon

Commented [61]: Definition of urgent category and penalties for abuse of such designation

i) Code of conduct

Objective: Define the policy requirements around:

1. How should a code of conduct (if any) be developed?
2. If ICANN and its contracted parties develop a code of conduct for third parties with legitimate interest, what features and needs should be considered?
3. Are there additional data flows that must be documented outside of what was documented in Phase 1?

Can a Code of Conduct model compliment or be used with what is implemented from EPDP-Phase 1 Recommendation #18?

Materials to review:

Description	Link	Required because
GDPR Article 40, Code of Conduct	https://gdpr-info.eu/art-40-gdpr/	
Art. 29 Working Party Letter to ICANN 11 April 2018	https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf	
Bird & Bird - Code of Conduct and Certification Reference Material (May 2017)	https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/43--guide-to-the-gdpr--codes-of-conduct-and-certifications.pdf?la=en	
Example: Cloud Providers Code of Conduct (CISPE) (January 2017)	https://cispe.cloud/code-of-conduct/	

Commented [62]: From IPC: again this section presupposes the use of an need for a code of conduct. suggest the use of a generic term.

Commented [63]: The term "acceptable use policy" is a better fit.

Commented [64]: developed, continuously evolved and enforced

Example: Cloud Providers Code of Conduct (EU Cloud) (November 2018)	https://eucoc.cloud/en/contact/request-the-eu-cloud-code-of-conduct.html	

Related mind map questions:

P1-Charter-c
c1) What rules/policies will govern users' access to the data?
c2) What rules/policies will govern users' use of the data once accessed?
c3) Who will be responsible for establishing and enforcing these rules/policies?
c4) What, if any, sanctions or penalties will a user face for abusing the data, including future restrictions on access or compensation to data subjects whose data has been abused in addition to any sanctions already provided in applicable law?
c5) What kinds of insights will Contracted Parties have into what data is accessed and how it is used?
c6) What rights do data subjects have in ascertaining when and how their data is accessed and used?
c7) How can a third party access model accommodate differing requirements for data subject notification of data disclosure?

Related EPDP Phase 1 Implementation: None.

Tasks:
- Determine full list of policy questions and deliberate each
- Determine possible solutions or proposed recommendation, if any
- Confirm all charter questions have been addressed and documented

Target date for completion: August

j) Terms of use / disclosure agreements / privacy policies

Objective: Define policy requirements around terms of use for third parties who seek to access nonpublic registration data:

- At a minimum, what required measures are needed to adequately safeguard personal data that may be made available to an accredited user/third party?
- What procedures should be established for accessing data?
- What procedures should be established for limiting the use of data that is properly accessed?
- Should separate Terms of Use be required for different user groups?
- Who would monitor and enforce compliance with Terms of Use?
- What mechanism would be used to require compliance with the Terms of Use?

Materials to review:

Description	Link	Required because
Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data - What would be the role of Terms of Use in a unified access model?	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-20aug18-en.pdf pages 14-16	

Related mind map questions:

P1-Charter-c
c1) What rules/policies will govern users' access to the data?
c2) What rules/policies will govern users' use of the data once accessed?
c3) Who will be responsible for establishing and enforcing these rules/policies?
c4) What, if any, sanctions or penalties will a user face for abusing the data, including future restrictions on access or compensation to data subjects whose data has been abused in addition to any sanctions already provided in applicable law?

TSG-Final-Q#4
Detail whether a particular category of Requestors or Requestors in general, can download logs of their activity.
TSG-Final-Q#10
Describe the conditions, if any, under which requests would be disclosed to CPs.
TSG-Final-Q#11
Provide legal analysis regarding liability of the operators of various components of the system.

TSG-Final-Q#12
Outline a procedure for fielding complaints about inappropriate disclosures and, accordingly, an Acceptable Use Policy

Related EPDP Phase 1 Implementation:

Tasks:

- Confirm definitions of key terms
- Determine full list of policy questions and deliberate each
- Determine possible solutions or proposed recommendation, if any
- Confirm all charter questions have been addressed and documented

Target date for completion: September

k) Retention and destruction of data

Objective: Establish minimum policy requirements for retention, deletion and logging of data retained for parties involved in the SSAD, including but limited to, gTLD registration data, user account information, transaction logs, and metadata such as date-and-time of requests

Materials to review:

Description	Link	Required because
GDPR Article 5(1)(e)	https://gdpr.algolia.com/gdpr-article-5	
Data retention in the TSG model	https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf page 26	

Related mind map questions:

P1-Charter-c
c2) What rules/policies will govern users' use of the data once accessed?

TSG-Final-Q#5
Describe data retention requirements imposed on each component of the system.

Related EPDP Phase 1 Implementation: Recommendation #15:
1. In order to inform its Phase 2 deliberations, the EPDP team recommends that ICANN Org, as a matter of urgency, undertakes a review of all of its active processes and procedures so as to identify and document the instances in which personal data is requested from a registrar beyond the period of the 'life of the registration'. Retention periods for specific data elements should then be identified, documented, and relied upon to establish the required relevant and specific minimum data retention expectations for registrars. The EPDP Team recommends community members be invited to contribute to this data gathering exercise by providing input on other legitimate purposes for which different retention periods may be applicable.

2. In the interim, the EPDP team has recognized that the Transfer Dispute Resolution Policy ("TDRP") has been identified as having the longest justified retention period of one year and has therefore recommended registrars be required to retain only those data elements deemed necessary for the purposes of the TDRP, for a period of fifteen months following the life of the registration plus three months to implement the deletion, i.e., 18 months. This retention is grounded on the stated policy stipulation within the TDRP that claims under the policy may only be raised for a period of 12 months after the alleged breach (FN: see TDRP section 2.2) of the Transfer Policy (FN: see Section 1.15 of TDRP). This retention period does not restrict the ability of registries and registrars to retain data elements provided in Recommendations 4 -7 for other purposes specified in Recommendation 1 for shorter periods.

3. The EPDP team recognizes that Contracted Parties may have needs or requirements for different retention periods in line with local law or other requirements. The EPDP team notes that nothing in this recommendation, or in separate ICANN-mandated policy, prohibits contracted parties from setting their own retention periods, which may be longer or shorter than what is specified in ICANN policy.

4. The EPDP team recommends that ICANN Org review its current data retention waiver procedure to improve efficiency, request response times, and GDPR compliance, e.g., if a Registrar from a certain jurisdiction is successfully granted a data retention waiver, similarly-situated Registrars might apply the same waiver through a notice procedure and without having to produce a separate application.

Tasks:

- Confirm definitions of key terms
- Determine full list of policy questions and deliberate each
- Determine possible solutions or proposed recommendation, if any
- Confirm all charter questions have been addressed and documented

Target date for completion: September

l) Financial sustainability

Objective: Ensure that all aspects of SSAD are financially sustainable. Consider how and by whom costs of SSAD implementation and management are borne.

- Determine if market inefficiencies existed prior to May 2018 and if any exist in a post EPDP-Phase 1 implemented world.
- Should contracted parties and or ICANN bear the cost of a standardized solution, even if the disclosure of registration data is considered in the public interest?
- If accreditation is a viable solution, should there be application fees associated, or should a fee structure be based on the type (tiered), size, or quantify of disclosures?
- Should or could data subjects be compensated for disclosures of their data?

Materials to review:

Description	Link	Required because

Related mind map questions: None

Related EPDP Phase 1 Implementation: None

Tasks:

- Confirm definitions of key terms
- Determine full list of policy questions and deliberate each
- Determine possible solutions or proposed recommendation, if any
- Confirm all charter questions have been addressed and documented

Target date for completion: TBD

Page 1: [1] Commented [6] **Alan Woods** **6/6/19 12:59:00 PM**

i'm sorry Brian, can you clarify what you are saying here? To be clear, for EVERY party outside of public authorities, or those empowered by law to have data disclosed to them, requests for disclosure, even in the SSAD, will always be 6(1)f and the will always attract the balancing test.

If you are referring to Law Enforcement (and other so empowered public authorities), should they even want to use the SSAD, must rely on 6(1)e , 6(1)c and perhaps 6(1)d. This is tempered by the requirements of 6(3) and they shall have to demonstrate the legal basis in EU or Member State law. I doubt 6(1)d will regularly rear it's head in our context as, it is an exceptionally high threshold of "vital interests" to overcome (imminent threat to life is the prevailing thought on this). Much easier for them to just invoke the powers granted them by Union or member state law.

Page 1: [2] Commented [7] **Alan Woods** **6/6/19 1:34:00 PM**

Mark S, I'm sorry can you clarify also.. what other legal basis? You note consent! I'm struggling with this , unless you are thinking that we get that consent on a case by case basis, upon receipt of a 3rd party request?

If you are contemplating that such consent can be obtained upon registration, then I think you will find strong disagreement. How could we ever establish that such a consent was fully informed, or that it was freely given? How could the registrar possibly communicate this to the registrant upon collection? How would you even log and monitor this? So I will as, much the same question I asked Brian, please provide details as to how any other legal basis for disclosure will apply here, other than 6(1)f? (for LEAs see comments above - but let's call a spade a spade here - your focus is not on LEA access here, but I you think so, I did cover that in my response to Brian K above)

in short I do not agree in flipping this, because it presupposes that 3rd parties somehow have a right to have data disclosed to them. Unless there is a specific legal obligation involved, or they are doing so in the public interest which is specifically under the powers granted to them by Union law or Member State law, they simply do not!

Page 1: [3] Commented [8] **mark svancarek** **6/6/19 1:46:00 PM**

There are two separate issues in your response. If an Office 365 subscriber tells us to view their registration data in order to verify that they own the domain name that they bring to their subscription, our viewing of it won't be 6(1)(f). The practical solution for conveying that subscriber request from us to a registrar is separate from the legal basis for us asking to get that data on their behalf.

Page 1: [4] Commented [9] **Alan Woods** **6/6/19 1:56:00 PM**

Mark, that is consent you have obtained, as a Data Controller (and indeed as a company providing service that you have deemed to require an element of such confirmation) in a separate data processing system. It's nothing to do with the the consent provided to a Registrar upon registration of a domain.

But I will concede that that's a pretty strong 6(1)f basis IMHO..... what's your legitimate business interest ... I am providing services to the data subject and I have consent from the data subject to get this data [provides confirmation of consent].

Page 1: [5] Commented [10] **Volker Greimann** **6/6/19 2:01:00 PM**

There will have to be granting, either by the CPs or by an entity the CPs outsource the granting to. The standardization is supposed to get rid of differences between CPS as much as possible,

but not the granting.