ICANN | GNSO

Generic Names Supporting Organization

Initial Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process

[Date]

Status of This Document

This is the Initial Recommendations Report of the GNSO Expedited Policy Development Process (EPDP) Team on the Temporary Specification for gTLD Registration Data Phase 2 that has been posted for public comment.

Preamble

The objective of this Initial Report is to document the EPDP Team's: (i) deliberations on charter questions, (ii) preliminary recommendations, and (iii) additional identified issues to consider before the Team issues its Final Report. The EPDP Team will produce its Final Report after its review of the public comments received in response to this report. The EPDP Team will submit its Final Report to the GNSO Council for its consideration.

Table of Contents

1 Executive Summary

On 17 May 2018, the ICANN Board of Directors (ICANN Board) adopted the Temporary Specification for generic top-level domain (gTLD) Registration Data[1] ("Temporary Specification"). The Temporary Specification provides modifications to existing requirements in the Registrar Accreditation and Registry Agreements in order to comply with the European Union's General Data Protection Regulation ("GDPR").[2] In accordance with the ICANN Bylaws, the Temporary Specification will expire on 25 May 2019.

On 19 July 2018, the GNSO Council initiated an Expedited Policy Development Process (EPDP) and chartered the EPDP on the Temporary Specification for gTLD Registration Data team. In accordance with the Charter, EPDP team membership was expressly limited. However, all ICANN Stakeholder Groups, Constituencies and Supporting Organisations interested in participating are represented on the EPDP Team.

During phase 1 of its work, the EPDP Team was tasked to determine if the Temporary Specification for gTLD Registration Data should become an ICANN Consensus Policy as is, or with modifications. This Initial Report concerns phase 2 of the EPDP Team's charter which covers: (i) discussion of a system for standardized access/disclosure to nonpublic registration data, (ii) issues noted in the Annex to the Temporary Specification for gTLD Registration Data ("Important Issues for Further Community Action"), and (iii) outstanding issues deferred from Phase 1, e.g., legal vs. natural persons, redaction of city field, et. al. For further details, please see here.

This Initial Report contains the preliminary recommendations of the EPDP Team and includes a set of questions for public review and comment. In the Initial Report, the EPDP Team also examined and made recommendations regarding:

[TBC]

The EPDP Team reached tentative agreement on many of these recommendations, but the Chair did not conduct a formal consensus call at this time. Team members did not reach agreement on some areas of discussion; where applicable, the Report describes the areas of disagreement and provides specific questions for public consideration and comment.

As a result of external dependencies and time constraints, this Initial Report does not include [all] priority 2 items. Once addressed, these are expected to be published in a separate Initial Report.

[1] Because the Temporary Specification is central to the EPDP Team's work, readers unfamiliar with the Temporary Specification may wish to read it before reading this Initial Report to gain a better understanding of and context for this Initial Report.
[2] The GDPR can be found at https://eur-lex.europa.eu/eli/reg/2016/679/oj; for information on the GDPR see, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/.

Following the publication of this Report, the EPDP Team will: (i) continue to seek guidance on legal issues from the European Data Protection Board and others, (ii) carefully review public comments received in response to this publication, (iii) continue to review the work-in-progress with the community groups the Team members represent, and (iv) carry on deliberations for the production of a Final Report that will be reviewed by the GNSO Council and, if approved, forwarded to the ICANN Board of Directors for approval as an ICANN Consensus Policy.

2 Overview of Preliminary Recommendations

In phase 2 of its work, this EPDP Team was chartered to address (i) a system for standardized access/disclosure to nonpublic registration data, (ii) issues noted in the Annex to the Temporary Specification for gTLD Registration Data ("Important Issues for Further Community Action"), and (iii) outstanding issues deferred from Phase 1, e.g., legal vs. natural persons, redaction of city field, et. al.

The EPDP Team will not finalize its responses to the charter questions and recommendations to the GNSO Council until it has conducted a thorough review of the comments received during the public comment period on this Initial Report. At this time, no formal consensus call has been taken on these responses and preliminary recommendations, but this Initial Report did receive the support of the EPDP Team for publication for public comment.[3] Where applicable, the Initial Report indicates where positions within the Team differ.

Notwithstanding the above, the EPDP Team is putting forward the following preliminary recommendations and related questions for community consideration:

[To be updated]

2.1 Conclusions and Next Steps

This Initial Report will be posted for public comment for [X] days. After the EPDP Team's review of public comments received on this Report, the EPDP Team will update and finalize this Report as deemed necessary for submission to the GNSO Council.

2.2 Other Relevant Sections of this Report

For a complete review of the issues and relevant interactions of this EPDP Team, the following sections are included within this Report:

- Background of the issues under consideration;
- Documentation of who participated in the EPDP Team's deliberations, including attendance records, and links to Statements of Interest as applicable;
- An annex that includes the EPDP Team's mandate as defined in the Charter adopted by the GNSO Council; and
- Documentation on the solicitation of community input through formal SO/AC and SG/C channels, including responses.

[3] Following a review of public comments, the EPDP Team will take a formal consensus call before producing its Final Report.

3 EPDP Team Approach

This Section provides an overview of the working methodology and approach of the EPDP Team. The points outlined below are meant to provide the reader with relevant background information on the EPDP Team's deliberations and processes and should not be read as representing the entirety of the efforts and deliberations of the EPDP Team.

3.1 Working Methodology

The EPDP Team began its deliberations for phase 2 on 2 May 2019. The Team agreed to continue its work primarily through conference calls scheduled once or more times per week, in addition to email exchanges on its mailing list. Additionally, the EPDP Team held three face-to-face meetings: the first set of face-to-face discussions took place at the ICANN65 Public Meeting in Marrakech, Morocco, followed by one dedicated set of face-to-face meetings at the ICANN headquarters in Los Angeles in September of 2019 and a third set of face-to-face discussions, which took place at the ICANN66 Public Meeting in Montreal, Canada. All of the EPDP Team's meetings are documented on its wiki workspace, including its mailing list, draft documents, background materials, and input received from ICANN's Supporting Organizations and Advisory Committees, including the GNSO's Stakeholder Groups and Constituencies.

The EPDP Team also prepared a Work Plan, which was reviewed and updated on a regular basis. In order to facilitate its work, the EPDP Team used a template to tabulate all input received in response to its request for Constituency and Stakeholder Group statements (see Annex B). This template was also used to record input from other ICANN Supporting Organizations and Advisory Committees and can be found in Annex C.

The EPDP Team held a community session at the ICANN66 Public Meeting in Montreal, during which it presented its methodologies and preliminary findings to the broader ICANN community for discussion and feedback.

3.2 Mind Map, Worksheets and Building Blocks

In order to ensure a common understanding of the topics to be addressed as part of its phase 2 deliberations, the EPDP Team mapped the topics using the following mind maps, which allowed for the regrouping and consolidation of topics (see mind map). This formed the basis for the subsequent development of the priority 1 and priority 2 worksheets (see worksheets) which the EPDP Team used to capture:

- Issue description / related charter questions
- Expected deliverable
- Required reading
- Briefings to be provided
- Legal questions
- Dependencies

- Proposed timing and approach

The EPDP Team Chair also put forward a number of working definitions to ensure consistent terminology and a shared understanding of terms used during the EPDP Team's deliberations (see working definitions).

Following the review of a number of real life use cases, the EPDP Team established a set of building blocks that the System for Standardized Access/Disclosure ("SSAD") would consist of, recognizing that a decision on the roles and responsibilities of the different parties involved may be influenced by both legal advice and guidance from the European Data Protection Board ("EDPB"). In the absence of this guidance, the EPDP Team established that there would be roughly three variations[4] of the SSAD:

1. Centralized model in which requests for access/disclosure are received through a central gateway, where the decision on whether to disclose data would be made by the entity responsible for managing the centralized gateway;
2. Hybrid model in which requests for access/disclosure are received through a central gateway, where the decision on whether to disclose data would remain with the relevant contracted party;
3. Decentralized model in which requests for access/disclosure would be received by the relevant contracted party and the decision on whether to disclose would be made by the relevant contracted party (status quo, but with newly-defined standardized requirements).

The Centralized model may have variations with respect to how data is returned to the requestor. For example, the central gateway may return the data via its system, or, alternatively, the contracted party may return the data directly to the requestor following instruction from the authorization provider.

3.3 Priority 1 and Priority 2 Topics

In order to organize its work, the EPDP Team agreed to divide its work into priority 1 and priority 2 topics. Priority 1 consists of the SSAD and all directly-related questions. Priority 2 includes the following topics:

- Display of information of affiliated vs. accredited privacy / proxy providers
- Legal vs. natural persons
- City field redaction
- Data retention
- Potential Office of the Chief Technology Officer Purpose
- Feasibility of unique contacts to have a uniform anonymized email address

[4] The EPDP Team recognizes that there are variations of these three models, but assumes that the requirements as outlined in the next section would be largely the same.

- Accuracy and WHOIS Accuracy Reporting System

The EPDP Team agreed that priority should be given to completing the deliberations for priority 1 items. It agreed, however, that where feasible, the Team would also endeavor to make progress on priority 2 items in parallel. As a result, a number of priority 2 items [update accordingly] have also been addressed in this Initial Report, but some topics remain outstanding due to external dependencies, and, as a result, these topics will be dealt with separately.

3.4 Legal Committee

Recognizing the complexity of many issues the EPDP Team was chartered to work through in Phase 2, the EPDP Team requested resources for the external legal counsel of Bird & Bird. To assist in preparing draft legal questions for Bird & Bird, EPDP Leadership chose to assemble a Legal Committee, comprised of one member from each SO/AC represented on the EPDP Team.

The Phase 2 Legal Committee worked together to review questions proposed by the members EPDP Team to ensure:

1. the questions were truly legal in nature, as opposed to a policy or policy implementation questions;
2. the questions were phrased in a neutral manner, avoiding both presumed outcomes as well as constituency positioning;
3. the questions were both apposite and timely to the EPDP Team's work; and
4. the limited budget for external legal counsel was used responsibly.

The Legal Committee presented all agreed-upon questions to the EPDP Team for its final sign-off before sending questions to Bird & Bird.

To date, the EPDP Team agreed to send four SSAD-related questions to Bird & Bird. The full text of the questions and executive summaries of the legal advice received in response to the questions can be found in Annex F.

3.5 Charter Questions

In addressing the charter questions, the EPDP Team considered both (1) the input provided by each group as part of the deliberations; (2) relevant input from phase 1; (3) the input provided by each group in response to the request for Early Input in relation to the specific charter questions; (4) the required reading identified for each topic in the worksheets, and (5) input provided by the EPDP Team's legal advisors, Bird & Bird.

4 EPDP Team Responses to Charter Questions & Preliminary Recommendations

The EPDP Team will not finalize its responses to the charter questions and recommendations to the GNSO Council until it has conducted a thorough review of the comments received during the public comment period on this Initial Report. Additionally, if the EPDP receives further guidance from the European Data Protection Board ("EDPB"), the EPDP Team will consider this guidance in its Final Report.[5] At the time of publication of this Report, no formal consensus call has been taken on these responses and preliminary recommendations; however, this Initial Report did receive the support of the EPDP Team for publication for public comment.[6] Where applicable, differing positions have been reflected in the Report.

4.1 System for Standardized Access/Disclosure to Non-Public Registration Data (SSAD)

In Annex A, further details are provided in relation to the approach and the materials that the EPDP Team reviewed in order to address the charter questions and develop the following preliminary recommendations.

As outlined in the previous section, the EPDP Team has established that there could be roughly three variations[7] of the SSAD:

1. Centralized model in which requests for access/disclosure are received through a central gateway, where the decision on whether to disclose data would be made by the entity responsible for managing the centralized gateway;
2. Hybrid model in which requests for access/disclosure are received through a central gateway, where the decision on whether to disclose data would remain with the relevant contracted party;
3. Decentralized model in which requests for access/disclosure would be received by the relevant contracted party and the decision on whether to disclose data would be made by the relevant contracted party (status quo, but with [newly-defined] standardized requirements).

The Centralized model may have variations with respect to how data is returned to the requestor. For example, the central gateway may return the data via its system, or, alternatively, the contracted party may return the data directly to the requestor following instruction from the authorization provider.

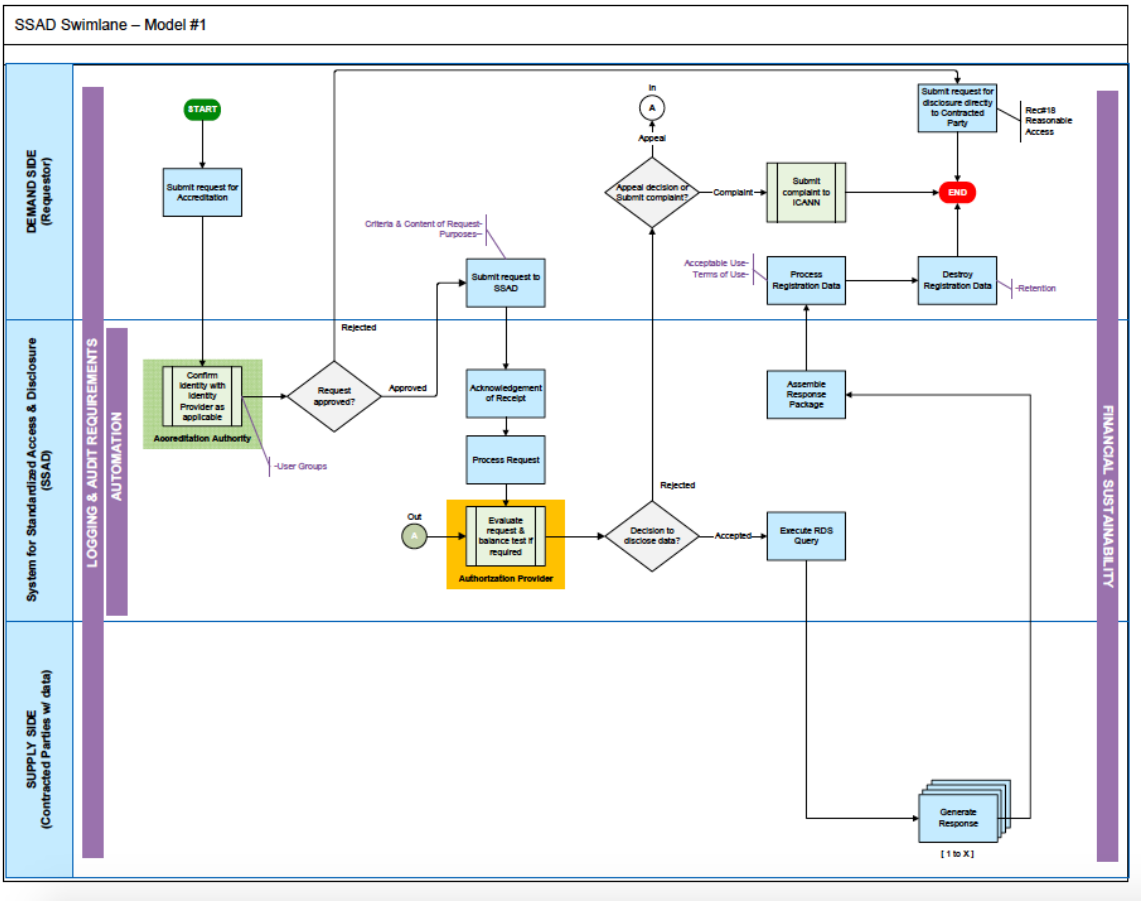
[5] See https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-stevens-25oct19-en.pdf and https://www.icann.org/en/system/files/files/unified-access-model-gtld-registration-data-25oct19-en.pdf

[6] Following a review of public comments, the EPDP Team will take a formal consensus call before producing its Final Report.

[7] The EPDP Team recognizes that there are variations within these three models, but assumes that the requirements as outlined in the next section would remain largely the same.

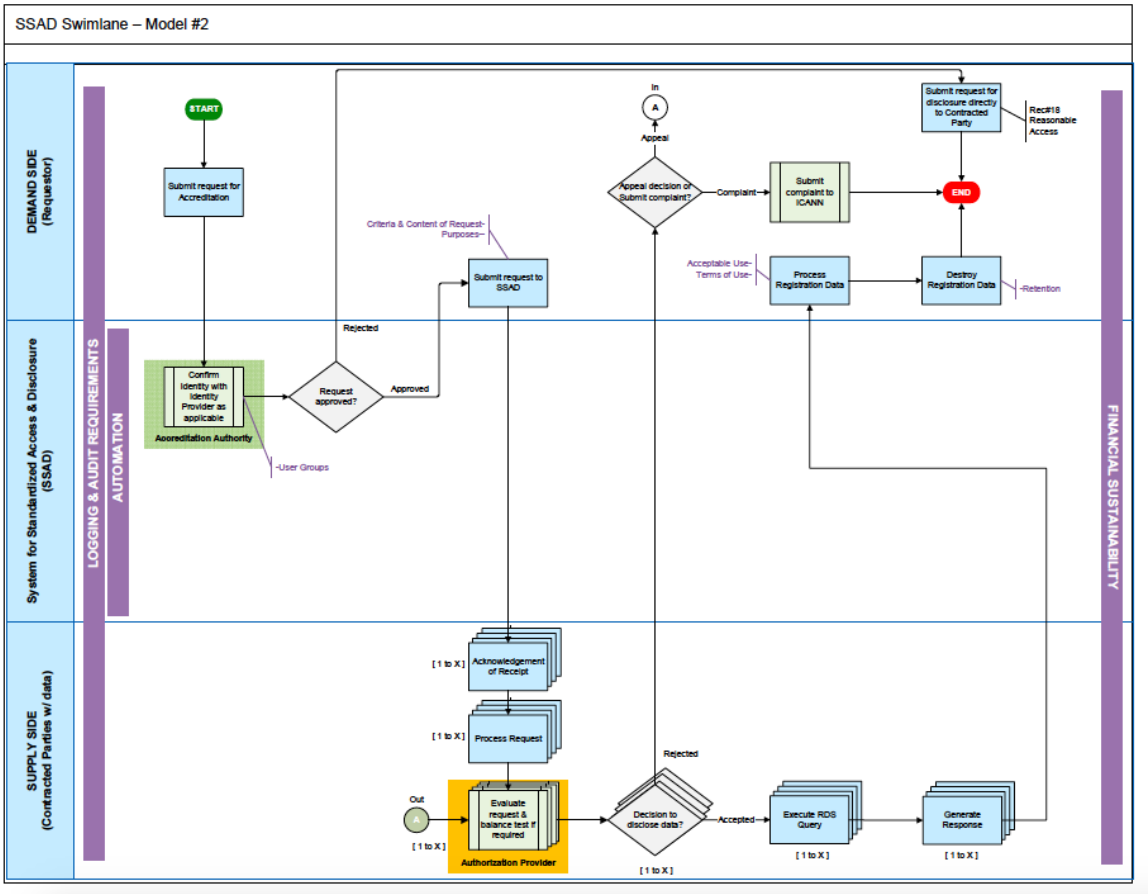
These three models have been visually represented hereunder[8]; the diagram highlights which aspects of the roles and responsibilities are expected to change depending on the chosen model.

Model 1:

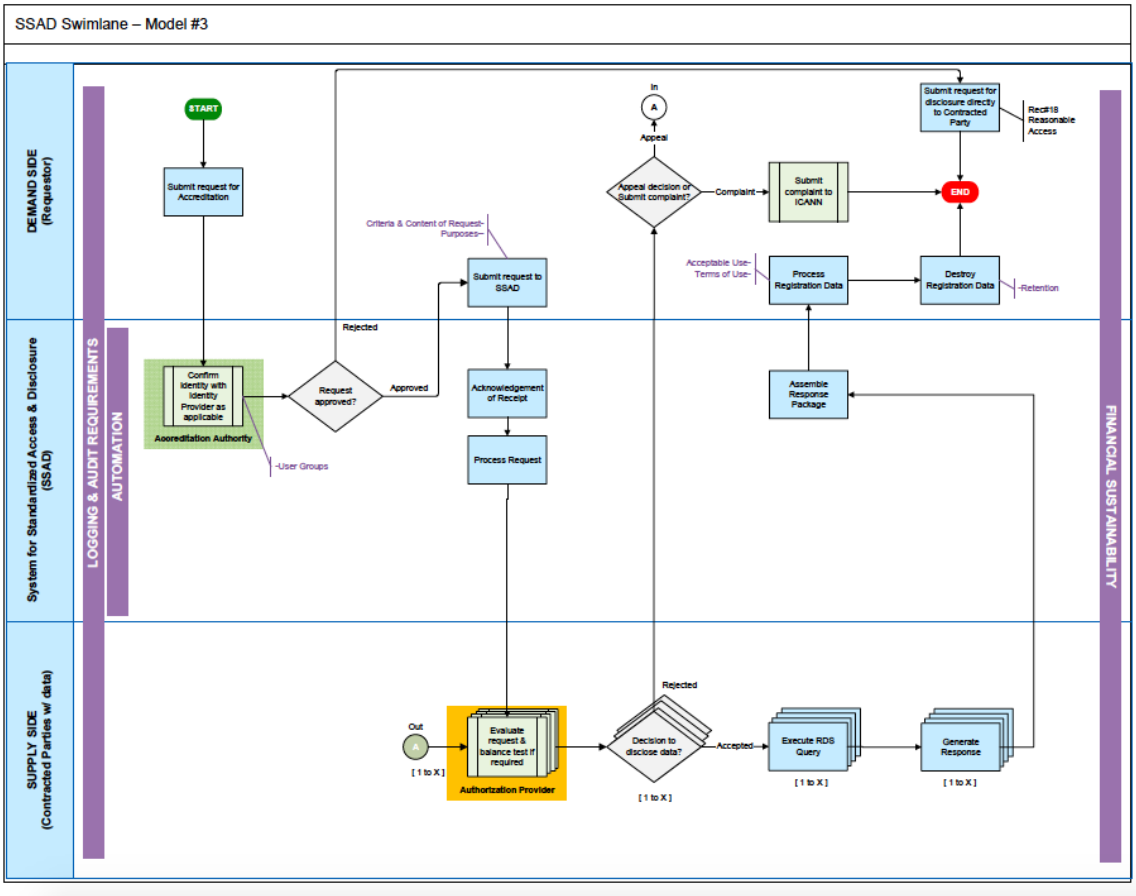


[8] For a standalone version, please see https://community.icann.org/x/BQZxBw.

Model 2:


SSAD Swimlane – Model #2
DEMAND SIDE (Requestor)
System for Standardized Access & Disclosure (SSAD)
SUPPLY SIDE (Contracted Parties w/ data)
LOGGING & AUDIT REQUIREMENTS
AUTOMATION
FINANCIAL SUSTAINABILITY
START
Submit request for Accreditation
Confirm Identity with Identity Provider as applicable
Accreditation Authority
-User Groups
Request approved?
Rejected
Approved
Criteria & Content of Request-Purposes-
Submit request to SSAD
[1 to X]
Acknowledgement of Receipt
[1 to X]
Process Request
Out
A
[1 to X]
Evaluate request & balance test if required
Authorization Provider
Rejected
Decision to disclose data?
[1 to X]
Accepted
Execute RDS Query
[1 to X]
Generate Response
[1 to X]
In
A
Appeal
Appeal decision or Submit complaint?
Complaint
Submit complaint to ICANN
END
Submit request for disclosure directly to Contracted Party
Rec#18 Reasonable Access
Acceptable Use-Terms of Use-
Process Registration Data
Destroy Registration Data
-Retention

Model 3:



As of this Report's publication, the EPDP Team has not yet decided on a conclusive model. This Report references terms such as the "entity receiving requests", the "authorization provider" and the "entity disclosing the data". Within this Report, the "authorization provider" means the entity responsible for making a determination on whether the data should be disclosed, which is one of the main areas of disagreement within the EPDP Team. Some members advocate for ICANN to take on this role, while others prefer Contracted Parties to remain responsible for making this determination. Some members of the EPDP Team are of the view that a centralized model will result in increased uniformity and predictability, while a decentralized model will likely result in increased inconsistency and decreased predictability. Nevertheless, the EPDP Team expects that most of the preliminary recommendations are applicable regardless of which model is ultimately chosen. However, where possible, the EPDP Team has indicated where a difference in the three models may result in a change in responsibility.

Below is a detailed breakdown of the underlying assumptions and policy recommendations that the EPDP Team is putting forward for community input.

4.2 ICANN Board and ICANN Org Input

In order to help inform its deliberations, the EPDP Team reached out to both the ICANN Board and ICANN Org "to understand the Board's position on the scope of operational responsibility and level of liability (related to decision-making on disclosure of non-public registration data) they are willing to accept on behalf of the ICANN organization along with any prerequisites that may need to be met in order to do so".

ICANN Org provided its response on 19 November 2019 noting in part that "ICANN org proposed that it could operate a gateway for authorized data to pass through. As noted above, the gateway operator does not make the decision to authorize disclosure. In the proposed model, the authorization provider would decide whether or not the criteria for disclosure are met. If a request is authorized and authenticated, the gateway operator would request the data from the contracted party and disclose the relevant data set to the requestor".

The ICANN Board provided its response on 20 November 2019 noting in part that "the Board has consistently advocated for the development of an access model for non-public gTLD registration data. If the EPDP Phase 2 Team's work results in a consensus recommendation that ICANN org take on responsibility for one or more operational functions within a SSAD, the Board would adopt that recommendation unless the Board determined, by a vote of more than two-thirds, that such a policy would not be in the best interests of the ICANN community or ICANN. Given the Board's advocacy for the development of an access model, and support for ICANN org's dialogue with the EDPB on a proposed UAM, it is likely that the Board would adopt an EPDP recommendation to this effect".

The EPDP Team will consider this input together with the feedback from the EDPB, once received; the EPDP Team will also consider the input received during the public comment period, to make a final determination of the division of roles and responsibilities in the SSAD.

4.3 SSAD Underlying Assumptions

The EPDP Team used the following underlying assumptions to develop the following preliminary policy recommendations. These underlying assumptions do not necessarily create new requirements for contracted parties; instead, the assumptions are designed to assist both the readers of this Initial Report and the ultimate policy implementers in understanding the intent and underlying assumptions of the EPDP Team in drafting this Report.

- The objective of the SSAD is to provide a predictable, transparent and accountable mechanism for the access/disclosure of non-public registration data.
- Compliance with the GDPR and other applicable data protection legislations for all parties involved underpins the SSAD.

- The mechanism chosen to ultimately implement the SSAD must have the ability to adhere to these policy principles and recommendations.

4.4 SSAD Preliminary Policy Recommendations

These preliminary recommendations should be reviewed in conjunction with the flow charts above outlining the three SSAD models to fully understand and appreciate the roles, responsibilities as well as requirements that are expected to apply in a given model.

Preliminary Recommendation #1. Accreditation[9]

Proposed working definitions used by the EPDP Team in its discussion of accreditation:

- **Accreditation** - An administrative action by which the accreditation authority declares that a user is approved to gain access to SSAD in a particular security configuration with a prescribed set of safeguards.
- **Accreditation Authority** - A management entity who has been designated to have the formal authority to "accredit" users of SSAD, i.e., to confirm and Verify the identity of the user (represented by an Identifier Credential) and assertions (or claims) associated with the Identity Credential (represented by Authorization Credentials).
- **Accreditation Authority Auditor** - Independent entity that is contracted by ICANN org to carry out auditing requirements as outlined in auditing preliminary recommendation.
- **Authentication** - The process or action of Validating the Identity Credential and Authorization Credentials of a Requestor.
- **Authorization** - A process for approving or denying disclosure non-public registration data.
- **Credential**
    - **"Identifier Credential":** A data object that is a portable representation of the association between an identifier and a unit of authentication information, and that can be presented for use in Validating an identity claimed by an entity that attempts to access a system. Example: [Username/Password], [OpenID credential], X.509 public-key certificate.
    - **"Authorization Credential"**: A data object that is a portable representation of the association between an Identifier Credential and one or more access authorizations, and that can be presented for use in Validating those authorizations for an entity that attempts such access. Example: [OAuth credential], X.509 attribute certificate.
- **De-accreditation of Accreditation Authority –** An administrative action by which ICANN org revokes the agreement with the accreditation authority following which it is no longer approved to operate as the accreditation authority.
- **Identity Provider -** Responsible for 1) Verifying the identity of a requestor and managing an Identifier Credential associated with the requestor and 2) Verifying and managing

[9] Note that accreditation is not referring to accreditation/certification as discussed in GDPR Article 42/43.

Authorization Credentials associated with the Identifier Credential. For the purpose of the SSAD, the Identity Provider may be the Accreditation Authority itself or it may rely on zero or more 3rd parties.

- **Revocation of User Credentials-** The event that occurs when an Identity Provider declares that a previously valid credential has become invalid.
- **Validate -** To test or prove the soundness or correctness of a construct. (Example: The Discloser will Validate the Identity Credential and Authorization Credentials as part of its Authorization process.)
- **Validation -** Establish the soundness or correctness of a construct.
- **Verify -** To test or prove the truth or accuracy of a fact or value. (Example: Identity Providers Verify the identity of the requestor prior to issuing an Identity Credential.)
- **Verification -** The process of examining information to establish the truth of a claimed fact or value.

The EPDP Team recommends that a policy for accreditation of SSAD users is established.

The following principles underpin the accreditation policy:

a) SSAD must only accept requests for access/disclosure from accredited organizations or individuals. However, accreditation requirements must accommodate any intended user of the system, including an individual or organization who makes a single request. The accreditation requirements for regular users of the system and a one-time user of the system may differ.
b) Both legal persons and/or individuals are eligible for accreditation. An individual accessing SSAD using the credentials of an accredited entity warrants that the individual is acting on the authority of the accredited entity.
c) The accreditation policy defines a single Accreditation Authority, run and managed by ICANN org. This Accreditation Authority may work with external or third-party Identity Providers that could serve as clearinghouses to Verify identity and authorization information associated with those requesting accreditation.
d) The decision to authorize disclosure of registration data, based on Validation of the Identity Credential, Authentication Credentials, and data as required in preliminary recommendation concerning criteria and content of requests, will reside with the registrar, ICANN, or whatever authorization provider the EPDP Team ultimately agrees on.

Benefits of Accreditation:

e) Verifying the Identity of the Requestor: The Accreditation Authority MUST verify the identity of the requestor, resulting in an Identity Credential.
f) Management of Authorization Credentials: The Accreditation Authority MUST verify and manage a set of dynamic assertions/claims associated with and bound to the Identity Credential of the requestor. This verification, performed by an Identity Provider, results in Authorization Credentials. Authorization Credentials convey information such as:
    - Assertion as to the purpose(s) of the request
    - Assertion as to the legal basis of the requestor

- Assertion that the user identified by the Identity Credential is affiliated with the Accreditation Authority
- Assertion regarding compliance with laws (e.g., storage, protection and retention/disposal of data)
- Assertion regarding agreement to use the disclosed data for the legitimate and lawful purposes stated
- Assertion regarding adherence to safeguards and/or terms of service and to be subject to revocation if they are found to be in violation
- Assertions regarding prevention of abuse, auditing requirements, dispute resolution and complaints process, etc.
- Assertions specific to the requestor – trademark ownership/registration for example
- Power of Attorney statements, when/if applicable.

g) Validation of Identity Credentials and Authorization Credentials, in addition to the information contained in the request, facilitate the decision of the authorization provider to accept or reject the Authorization of an SSAD request. For the avoidance of doubt, the presence of these credentials alone DOES NOT result in or mandate an automatic access / disclosure authorization. However, the ability to automate access/disclosure authorization decision making is possible under certain circumstances.

h) Defines a base line "code of conduct" that establishes a set of rules that contribute to the proper application of data protection laws - including the GDPR - for the ICANN community, including:

- A clear and concise explanatory statement.
- A defined scope that determines the processing operations covered (the focus for SSAD would be on the Disclosure operation.)
- Mechanism that allow for the monitoring of compliance with the provisions.
- Identification of an Accreditation Body Auditor (a.k.a. monitoring body) and definition of mechanism(s) which enable that body to carry out its functions.
- Description as to the extent a "consultation" with stakeholders has been carried out.
- Etc.

The accreditation authority:

i) MUST have a uniform baseline application procedure and accompanying requirements for all applicants requesting accreditation, including:

- Definition eligibility requirements for accredited users
- Identity Validation, Procedures
- Identity Credential Management Policies: lifetime/expiration, renewal frequency, security properties (password or key policies/strength), etc.
- Identity Credential Revocation Procedures: circumstances for revocation, revocation mechanism(s), etc. [see also "Accredited User Revocation & abuse section below]
- Authorization Credential Management: lifetime/expiration, renewal frequency, etc.

- NOTE: requirements beyond the baseline listed above may be necessary for certain classes of requestors.

j) MUST define a dispute resolution and complaints process.

k) MUST be audited by an auditor on a regular basis. Should the Accreditation Authority be found in breach of the accreditation policy and requirements, it will be given an opportunity to address the breach, but in cases of repeated failure, a new Accreditation Authority must be identified or created. Additionally, accredited entities MUST be audited for compliance with the accreditation policy and requirements on a regular basis; (Note: detailed information regarding auditing requirements can be found in the Auditing preliminary recommendation).

l) MAY develop user groups / categories to facilitate the accreditation process as all requestors will need to be accredited, and accreditation will include identity verification.

m) MUST report publicly and on a regular basis on the number of accreditation requests received, accreditation requests approved/renewed, accreditations denied, accreditations revoked and information about the identity providers it is working with.

Accredited User Revocation & Abuse:

n) Revocation, within the context of the SSAD, means the Accreditation Authority can revoke the accredited user's status as an accredited user of the SSAD. A non-exhaustive list of examples where revocation may apply include 1) the accredited user's violation of the code of conduct, 2) the accredited user's abuse of the system, 3) a change in affiliation of the accredited user, or 4) where prerequisites for accreditation no longer exist.

o) A mechanism to report abuse committed by an accredited user must be provided by SSAD. Reports must be relayed to the Accreditation Authority for handling.

p) The revocation policy for individuals/entities should include graduated penalties. In other words, not every violation of the system will result in Revocation; however, Revocation may occur if the Accreditation Authority determines that the accredited individual or entity has materially breached the conditions of its accreditation and failed to cure based on: a) a third-party complaint received; b) results of an audit or investigation by the Accreditation Authority or auditor; c) any misuse or abuse of privileges afforded; d) repeated violations of the accreditation policy. In the event there is a pattern or practice of abusive behavior within an entity, the credential for the entity could be suspended or revoked as part of a graduated sanction.

q) Revocation will prevent re-accreditation in the future absent special circumstances presented to the satisfaction of the Accreditation Authority.

De-authorization of Identity Providers

r) The authorization policy for Identity providers should include graduated penalties. In other words, not every violation of the policy will result in De-authorization; however, De-authorization may occur if it has been determined that the Identity Provider has materially breached the conditions of its contract and failed to cure based on: a) a third-party complaint received; b) results of an audit or investigation by the Accreditation

Auditor or auditor; c) any misuse or abuse of privileges afforded; d) repeated violations of the accreditation policy. Depending upon the nature and circumstances leading to the de-authorization of an Identity Provider, some or all of its outstanding credentials may be revoked or transitioned to a different Identity Provider.

Accredited entities or individuals:

s) MUST agree to:
- only use the data for the legitimate and lawful purpose stated;
- the terms of service, in which the lawful uses of data are described;
- prevent abuse of data received;
- [cooperate with any audit or information requests as a component of an audit;]
- be subject to de-accreditation if they are found to abuse use of data or accreditation policy / requirements;
- store, protect and dispose of the gTLD registration data in accordance with applicable law;
- only retain the gTLD registration data for as long as necessary to achieve the purpose stated in the disclosure request.

t) Will not be restricted in the number of SSAD requests that can be submitted at a time, except where the accredited entity poses a demonstrable threat to the SSAD. It is understood that possible limitations in SSAD's response capacity and speed may apply. For further details see the response requirements preliminary recommendation.

Fees:
The accreditation service should be part of a cost-recovery system. For further details, see the financial sustainability preliminary recommendation.

Implementation Guidance

In relation to accreditation, the EPDP Team provides the following implementation guidance:

a) Recognized, applicable, and well-established organizations could support the Accreditation Authority as an Identity Provider and/or Verify information. Proper vetting must take place if any such reputable and well-established organizations are to collaborate with the Accreditation Authority.
b) Examples of additional information the Accreditation Authority or Identity Provider may require an applicant for accreditation to provide could include:
- a business registration number and the name of the authority that issued this number (if the entity applying for accreditation is a legal person);
- information asserting trademark ownership.

Auditing / logging by Accreditation Authority and Identity Providers

c) The accreditation/verification activity (such as accreditation request, information on the basis of which the decision to accredit or verify identity was made) will be logged by the Accreditation Authority and Identity Providers.
d) Logged data shall only be disclosed, or otherwise made available for review, by the Accreditation Authority or Identity Provider, where disclosure is considered necessary to a) fulfill or meet an applicable legal obligation of the Accreditation Authority or Identity Provider; b) carry out an audit under this policy or; c) to support the reasonable functioning of SSAD and the accreditation policy.

See also auditing and logging preliminary recommendations for further details.

Preliminary Recommendation #2. Accreditation of entities carrying out a public policy task

[TBC – proposed language to be provided by GAC team members]

Preliminary Recommendation #3. Criteria and Content of Requests
The EPDP Team recommends that each SSAD request must include, at a minimum, the following information:

a) Domain name pertaining to the request for access/disclosure;
b) Identification of and information about the requestor (including, requestor's accreditation status, if applicable, the nature/type of business entity or individual, Power of Attorney statements, where applicable and relevant);
c) Information about the legal rights of the requestor specific to the request 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?);
d) Affirmation that the request is being made in good faith and that data received (if any) will be processed lawfully and only in accordance with the justification specified in (c);
e) A list of data elements requested by the requestor, and why the data elements requested are adequate, relevant and limited to what is necessary.

The objective of this recommendation is to allow for the standardized submission of requested data elements, including any supporting documentation.

Preliminary Recommendation #4. Third Party Purposes/Justifications

[As identified in the preliminary recommendation relating to criteria and content of requests, each request must include information about the legal rights of the requestor specific to the request and/or 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? The EPDP Team expects that over time, the entity responsible for receiving requests will be able to identify certain patterns that could result in the development of a preset list of rationales

and/or justifications that a requestor can select from, while always maintaining the option for the requestor to provide this information in free form".]

Preliminary Recommendation #5. Receipt of acknowledgement

The EPDP Team recommends that, consistent with the EPDP Phase 1 recommendations, the response time for acknowledging receipt of a SSAD request should be without undue delay, but not more than two (2) business days from receipt, unless (i) shown circumstances do not make this possible or (ii) the SSAD is implemented using technologies which allow instantaneous responses to disclosure requests, in which case, the acknowledgement of receipt must be instantaneous.

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

Preliminary Recommendation #6. Authorization Provider

1. The authorization provider MUST review every request on its merits and MUST NOT disclose data on the basis of accredited user category alone. For the avoidance of doubt, automated review is not explicitly prohibited where it is both legally and technically permissible.
2. The authorization provider MUST confirm that all required information as per building block a) 'criteria and content of requests' is provided. Should the authorization provider determine that the request is incomplete, the authorization provider must reply to the requestor with an incomplete request response, detailing which required data is missing, and provide an opportunity for the requestor to amend its request. [Note: this confirmation could also be the responsibility of the central gateway manager if the manager is not the same entity as the authorization provider.
3. While the requestor will have the ability to identify the lawful basis under which it expects the authorization provider to disclose the data requested, the authorization provider must make the final determination of the appropriate lawful basis.
4. The authorization provider should make a threshold determination (without processing the underlying data) about whether the requestor has established an interest in the disclosure of personal data. The determination should consider the elements:
    - Is the identity of the requestor clear/verified?
    - Has the requestor provided a legitimate interest or other lawful basis in processing the data?
    - Are the data elements requested necessary to the requestor's stated purpose?
        - Necessary means more than desirable but less than indispensable or absolutely necessary.
    - Using the guidance provided in Preliminary Recommendation 3 (User Groups) and/or 5 (Purposes) about the usefulness and necessity of data elements, the authorization provider should determine whether Are the data elements requested are limited and reasonable to achieve the requestor's stated purpose?

- Each request should be evaluated individually (i.e. each submission should contain a request for data related to a single domain. If a submission relates to multiple domains, each must be evaluated individually.).
- In addition, each data element in a request should be evaluated individually.

If the answer to any of the above questions is no, the authorization provider may deny the request, or require further information from the requestor before proceeding to paragraph 6 below.

5. The authorization provider may evaluate the underlying data requested once the validity of the request is determined under paragraph 4 above. The purpose of paragraph 5 is to determine whether the paragraph 6 [meaningful human review] is required. The authorization provider's review of the underlying data should assess at least:
   - Does the data requested contain personal data?
     - If no personal data, no further balancing required.
   - If the requested data contains personal data the authorization provider should consider if the balancing test, similar to the requirements under GDPR's 6.1.f, as described in paragraph 6 below is applicable and proceed accordingly.
6. The authorization provider should evaluate at least the following factors to determine whether the legitimate interest of the requestor is not outweighed by the interests or fundamental rights and freedoms of the data subject. No single factor is determinative; instead the authorization provider should consider the totality of the circumstances outlined below:
   - **Assessment of impact**. Consider the direct impact on data subjects as well as any broader possible consequences of the data processing (e.g., triggering legal proceedings). Whenever the circumstances of the disclosure request or the nature of the data to be disclosed suggest an increased risk[10] for the data subject affected, this shall be taken into account during the decision-making.
   - ***Nature of the data***. Consider the level of sensitivity of the data as well as whether the data is already publicly available.
   - ***Status of the data subject***. Consider whether the data subject's status increases their vulnerability (e.g., children, other protected classes)
   - ***Scope of processing***. Consider information from the disclosure request or other relevant circumstances that indicates whether data will be [securely] held (lower risk) versus publicly disclosed, made accessible to a large number of persons, or combined with other data (higher risk), .[provided that this is not intended to prohibit public disclosures for legal actions or administrative dispute resolution proceedings such as the UDRP or URS].
   - ***Reasonable expectations of the data subject***. Consider whether the data subject would reasonably expect their data to be processed/disclosed in this manner.

[10] [include reference to relevant GDPR provision]

- ***Status of the controller and data subject***. Consider negotiating power and any imbalances in authority between the controller and the data subject.
- ***Legal frameworks involved***. Consider the jurisdictional legal frameworks of the requestor, Contracted Party/Parties, and the data subject, and how this may affect potential disclosures.

If, based on consideration of the above factors, the authorization provider determines that the requestor's legitimate interest is not outweighed by the interests or fundamental rights and freedoms of the data subject, the data **shall** be disclosed. The rationale for the approval should be documented.

If, based on consideration of the above factors, the authorization provider determines that the requestor's legitimate interest is outweighed by the interests or fundamental rights and freedoms of the data subject, the request may be denied. The rationale for the denial MUST be documented and MUST be communicated to the requestor, with care taken to ensure that no personal data is revealed to the requestor within this explanation.

7. The application of the balancing test and factors considered in paragraph 6 should be revised as appropriate to address applicable case law interpreting GDPR, guidelines issued by the EDPB or revisions to GDPR that may occur in the future.

Implementation Guidance

1. As noted in paragraph 4 above, in situations where the requestor has provided a legitimate interest for its request for access/disclosure, the authorization provider should consider the following:
    - Interest must be specific, real, and present rather than vague and speculative.
    - An interest is generally legitimate so long as it can be pursued consistent with data protection and other laws.
    - Examples of legitimate interests include: (i) enforcement of legal claims; (ii) prevention of fraud and misuse of services; and (iii) physical, IT, and network security.

Preliminary Recommendation #7. Response Requirements

Consistent with the EPDP Phase 1 recommendations, the EPDP Team recommends that:

a) The entity receiving the access/disclosure request must confirm[11] that all required information as per the preliminary recommendation 'criteria and content of requests' is provided. Should the entity receiving the access/disclosure request establish that the request is incomplete, the entity receiving the access/disclosure request must provide an opportunity for the requestor to amend and resubmit its request.

[11] It is the expectation that the initial review of the completeness of requests is done automatically with the system not accepting the request until all requested data has been provided.

b) Following confirmation that the request is syntactically correct and that all required information has been provided, the entity receiving the access/disclosure request must immediately and synchronously respond with an acknowledgement response.
c) The entity responsible for responding to the access/disclosure request must provide a disclosure response without undue delay, unless there are exceptional circumstances. Such exceptional circumstances may include the overall number of requests received if the number far exceeds the established SLAs. SSAD requests that meet the automatic response criteria must receive an automatic disclosure response. For requests that do not meet the automatic response criteria, a response must be received within a timeframe that is to be determined.[12]
d) 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). Additionally, in its response, the entity receiving the access/disclosure request must include information on how public registration data can be obtained.
e) A separate accelerated timeline will be recommended for the response to 'Urgent' SSAD Requests, those Requests for which evidence is supplied to show an immediate need for disclosure. The criteria to determine whether it concerns an urgent request are limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation.

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 its request was denied erroneously, a complaint should be filed with ICANN Compliance. ICANN Compliance must either compel disclosure or confirm that the denial was appropriate. If Contracted Parties are ultimately responsible for the decision to disclose data, ICANN Compliance should be prepared to investigate complaints regarding disclosure requests under its standard enforcement processes.

Implementation Guidance:

a) The entity receiving the access/disclosure request must confirm that the request is syntactically correct, including proper and valid Authentication and Authorization Credentials. Should the entity receiving the access/disclosure request establish that the request is syntactically incorrect, the entity receiving the access/disclosure request must

[12] Some members of the EPDP proposed that a disclosure response should be returned 1 calendar day for urgent requests and preferably within 7 calendar days for all other requests, others expressed concern about the implementability of these timeframes for non automated requests. The EPDP Team will review the timeframe further once it has made a determination of whom will be the authorization provider.

reply with an error response to the requestor detailing the errors that have been detected.

b) Should the entity receiving the access/disclosure request establish that the request is incomplete, the entity receiving the access/disclosure request must reply with an incomplete request response to the requestor detailing which data required by policy is missing, providing an opportunity for the requestor to amend its request.
c) Typically the acknowledgement response will include a "ticket number" or unique identifier to allow for future interactions with the SSAD.
d) An example of online critical infrastructure includes root servers; an example of offline critical infrastructure includes bridges. [examples to be provided by the EPDP Team]

Preliminary Recommendation #8. Acceptable Use Policy

The EPDP Team recommends that the following requirements are applicable to the requestor and must be confirmed by [TBC] and subject to an enforcement mechanism. For the avoidance of doubt, every request does not have to go through an enforcement procedure; the enforcement mechanism may, however, be triggered in the event of apparent misuse.

The requestor:

a) Must only request data from the current RDS data set (no historic data);
b) Must, for each and every unique request for RDS data, provide representations of the corresponding purpose and lawful basis for the processing, which will be subject to auditing (see the auditing preliminary recommendation for further details);
c) MAY request data from the SSAD for multiple purposes per request, for the same set of data requested;
d) For each stated purpose must provide (i) representation regarding the intended use of the requested data and (ii) representation that the requestor will only process the data for the stated purpose(s). These representations will be subject to auditing (see auditing preliminary recommendation further details);
e) Must handle the data subject's personal data in compliance with applicable law (see auditing preliminary recommendation for further details).

The EPDP Team recommends that the following requirements are applicable to the entity disclosing the data and must be confirmed by [TBC] and subject to an enforcement mechanism. For the avoidance of doubt, every response does not have to go through an enforcement procedure; the enforcement mechanism may, however, be triggered in the event of apparent misuse.

The entity disclosing the data:

a) Must only disclose the data requested by the requestor;
b) Must return current data or a subset thereof in response to a request (no historic data);
c) Must process data in compliance with applicable law;

d) Must log requests;
e) Where required by applicable law, must perform a balancing test before processing the data;
f) Must disclose to the Registered Name Holder (data subject), on reasonable request, confirmation of the processing of personal data relating to them, per applicable law;
g) Where required by applicable law, must provide mechanism under which the data subject may exercise its right to erasure;
h) Confidentiality of disclosure requests – Data controllers of RDS data must make it clear to data subjects the types of entities/third parties which may process their data. Upon a request from a data subject the exact processing activities of their data within the SSAD, should be disclosed as soon as reasonably feasible. However the nature of legal investigations or procedures may require SSAD and/or the disclosing entity keep the nature or existence of these requests confidential from the data subject. Confidential requests can be disclosed to data subjects in cooperation with the requesting authority, [and] [or] in accordance with the data subject's rights under applicable law.[13]

Preliminary Recommendation #9. Query Policy

The EPDP Team recommends that the entity disclosing the data:

a) Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system;
b) May take measures to limit the number of requests that are submitted by the same requestor if it is demonstrated that the requests are of an abusive* nature;

*"Abusive" use of SSAD may include (but is not limited to) the detection of one or more of the following behaviors/practices:

1. High volume automated submissions of malformed or incomplete requests.
2. High volume automated duplicate requests that are frivolous or vexatious.
3. Use of false, stolen or counterfeit credentials to access the system.
4. Storing/delaying and sending high-volume requests causing the SSAD or other parties to fail SLA performance. When investigating abuse based on this specific behavior, the concept of proportionality should be considered.

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

[13] The EPDP Team may reconsider this requirement once there is clarity on who will be the entity disclosing the data.

c) MUST respond only to requests for a specific domain name for which non-public registration data is requested to be disclosed and MUST examine each request on its own merits.

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

a) Unless otherwise required or permitted, not allow bulk access, wildcard requests, [reverse lookups[14]], nor boolean search capabilities.
b) Have the capacity to handle the expected number of requests in alignment with the SLAs established
c) Only return current data (no data about the domain name registration's history);
d) Receive a specific request for every individual domain name (no bulk access);
e) 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).

Preliminary Recommendation #10. Terms of use

The EPDP Team recommends that appropriate agreements, such as terms of use for the SSAD, a privacy policy and a disclosure agreement are put in place that take into account the recommendations from the other preliminary recommendations. These agreements are expected to be developed and negotiated by the parties involved in SSAD, taking the below implementation guidance into account.

Implementation guidance:

Privacy Policy

The EPDP recommends, at a minimum, the privacy policy shall include:

- Relevant data protection principles, for example,
- The type(s) of personal data processed
- How and why the personal data is processed, for example,
    - verifying identity
    - communicating service notices
- How long personal data will be retained
- The types of third parties with whom personal data is shared
- Where applicable, details of any international data transfers/requirements thereof
- Information about the data subject rights and the method by which they can exercise these rights
- Notification of how changes to the privacy policy will be communicated

[14] The EPDP Team is expected to request legal guidance on the issue of reverse lookups. Based on that input, this recommendation will be updated accordingly.

Further consideration should be given during implementation whether updates to the RAA are necessary to ensure compliance with these recommendations.

Terms of Use

The EPDP recommends, at a minimum, the terms of use shall address:

- Indemnification of the disclosing party and ICANN.
- Data request requirements
- Logging requirements
- Ability to demonstrate compliance
- Applicable prohibitions

Disclosure agreements

The EPDP recommends, at a minimum, disclosure agreements shall address:

- Use of the data for the purpose indicated in the request
- Requirements for use of data for a new purpose other than the one indicated in the request
- Retention of data
- Lawful use of data

Preliminary Recommendation #11. Retention and Destruction of Data

The EPDP Team recommends that requestors must confirm that they will store, protect and dispose of the gTLD registration data in accordance with applicable law. Requestors must retain only the gTLD registration data for as long as necessary to achieve the purpose stated in the disclosure request.

Preliminary Recommendation #12. Financial Sustainability

The EPDP Team recommends that, in considering the costs and financial sustainability of SSAD, one needs to distinguish between the development and operationalization of the system and the subsequent running of the system.

The EPDP Team expects that the costs for developing, deployment and operationalizing the system, similar to the implementation of other adopted policy recommendations, to be initially borne by ICANN org, Contracted Parties and other parties that may be involved. It is the EPDP Team's expectation that the SSAD will ultimately result in equal or lesser costs to Contracted Parties compared to manual receipt and review of requests. When implementing the SSAD, an unreasonable burden on smaller operators should be avoided.

The subsequent running of the system is expected to happen on a cost recovery basis whereby historic costs may be considered. For example, if the SSAD includes an accreditation framework under which users of the SSAD could become accredited, the costs associated with becoming accredited would be borne by those seeking accreditation. Similarly, some of the cost of running the SSAD may be offset by charging fees to the users of the SSAD.

The EPDP Team recognizes that the fees associated with using the SSAD may differ for users based on cost causation.

Under no circumstances should data subjects be expected to foot the bill for having their data disclosed to third parties; beneficiaries and users of the SSAD should bear the costs of maintaining this system.

The SSAD should not be considered a business opportunity or profit-generating platform; neither should operational costs be shifted onto ICANN (which then flows to the Contracted Party and thus to Registrants) or directly to Registrants or Contracted Parties. It is crucial to ensure that any payments in the SSAD are related to operational costs and are not simply an exchange of money for non-public registration data.

In relation to the accreditation framework:

a) Accreditation applicants may be charged a to-be-determined non-refundable fee proportional to the cost of validating an application.
b) Rejected applicants may re-apply, but the new application(s) will be subject to the application fee.
c) Fees are to be established by the accreditation authority.
d) Accredited users and organizations must renew their accreditation periodically.

[The fee structure as well as the renewal period is to be determined in the implementation phase, following the principles outlined above. The EPDP Team recognizes that it may not be possible to set the exact fees until the actual costs are known. The EPDP Team also recognizes that the accreditation fee structure may need to be reviewed over time.

The EPDP Team will further consider whether the resubmission of a request will be treated as a new request from a cost/fee perspective.

Implementation guidance:
The EPDP Team has requested input from ICANN Org concerning the expected costs of developing, operationalizing and maintaining the three different models. Based on the feedback received, the EPDP Team may develop further guidance in relation to the financial sustainability of SSAD.]

Preliminary Recommendation #13. Automation

The EPDP Team acknowledges that full automation of the SSAD may not be possible, but recommends that the SSAD [should, must or may] be automated where technically feasible and legally permissible[15]. Additionally, in areas where automation is not both technically feasible and legally permissible, the EPDP Team recommends standardization as the baseline objective.

For example, the EPDP Team expects that aspects of the SSAD such as intake of requests, credential check, request submission validation (format & completeness, not content) could be automated, while it may not be possible to completely automate request review and disclosure.

The SSAD must allow for the automation of syntax checking of incoming requests, resulting in an automatic response that indicates the errors to the requestor. This automation addresses the risk of filling up the request queues of the discloser with malformed requests.

The SSAD must allow for the automation of checking that the contents of a request is complete, per policy, resulting in an automatic response that provides details explaining what elements are incomplete. This automation allows for the discloser to indicate - without human intervention - if any additional information is required per policy and enables the requestor to address the error.

The SSAD must allow for the automation of an immediate and synchronous response that indicates the receipt of a valid request and some indication that it will be processed. Typically, such responses include a "ticket number" or some kind of unique ID to allow for future queries (status, updates, deletion, etc.). This automation allows for efficient queue management on the discloser's side and assists in ensuring the principal of "predictability" is met.

The SSAD [must or should] allow for automation of the processing of well-formed, valid, complete, properly-identified requests from accredited users with some limited and specific set of legal basis and data processing purposes which are yet to be determined. These requests MAY be automatically processed and result in the disclosure of non-public RDS data without human intervention.

Preliminary Recommendation #14. Logging

The EPDP Team expects that the appropriate logging procedures are put in place to facilitate the auditing procedures outlined in these recommendations. These logging requirements will cover the following:

- Accreditation authority
- Identity provider
- Activity of accredited users such as login attempts, queries

[15] EPDP Team to revisit this language once the decision of who will be the authorization provider is made.

- What queries and disclosure decision(s) are made[16]

The EPDP Team recommends:

a) The activity of all SSAD entities will be logged. (for further details, please see the implementation guidance below).
b) Logs will include a record of all queries and all items necessary to audit any decisions made in the context of SSAD.
c) Logs must be retained for a period sufficient for auditing and complaint resolution purposes, taking into account statutory limits related to complaints against the controller.
d) Logs must be retained in a commonly used, structured, machine-readable format accompanied by an intelligible description of all variables.
e) Logged data will remain confidential and must be disclosed in the following circumstances:
    i. In the event of a claim of misuse, logs may be requested for examination by an accreditation authority or dispute resolution provider.
    ii. Logs should be further available to data protection authorities, ICANN, and the auditing body.[17]
    iii. When mandated as a result of due legal process, including relevant supervisory authorities, as applicable.
    iv. General technical operation to ensure proper running of the system.

Implementation guidance:

At a minimum, the following events must be logged

- Logging related to the Identity Provider
    - Details of incoming requests for Accreditation
    - Results of processing requests for Accreditation, e.g., issuance of the Identity Credential or reasons for denial
    - Details of Revocation Requests
    - Indication when Identity Credentials and Authorization Credentials have been Validated.
- Logging related to the entity that receives the requests
    - Information related to the contents of the query itself.
    - Results of processing the query, including changes of state (e.g., received, pending, in-process, denied, approved, approved with changes)
- Logging related to the entity Authorizing the request

[16] Note, EPDP Team to review at a later stage as the ability for SSAD to log this information depends on who is the entity that makes the disclosure decision
[17] Note, EPDP Team to review at a later stage as there is a question of the set up of the system of whether or not the Ry and RR as Controllers (where liability remains with them) may require access to the logs for them to engage in audit, or answer Data Subject requests.

- Request Response details, e.g., Reason for denial, Notice of approval and data elements released.

Preliminary Recommendation #15. Audits

The EPDP Team expects that the appropriate auditing processes and procedures are put in place to ensure appropriate monitoring and compliance with the requirements outlined in these recommendations.

As part of any audit, the auditor MUST be subject to reasonable confidentiality obligations with respect to proprietary processes and personal information disclosed during the audit.

More specifically:

Audits of the Accrediting Authority

If ICANN outsources the accreditation authority function to a qualified third party, the accrediting authority MUST be audited periodically to ensure compliance with the policy requirements as defined in the accreditation preliminary recommendation. Should the accreditation authority be found in breach of the accreditation policy and requirements, it will be given an opportunity to cure the breach, but in cases of repeated non-compliance or audit failure, a new accreditation authority must be identified or created.

Any audit of the accreditation authority shall be tailored for the purpose of assessing compliance, and the auditor MUST give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data, and other information requested.

As part of such audits, the accreditation authority shall provide to the auditor in a timely manner all responsive documents, data, and any other information necessary to demonstrate its compliance with the accreditation policy.

If ICANN serves as the accreditation authority, existing accountability mechanisms are expected to address any breaches, noting that in such an extreme case, requirements for other entities involved in SSAD may be temporarily lifted until a confirmed breach has been addressed.

Audits of Identity Provider(s)

Identity Providers MUST be audited periodically to ensure compliance with the policy requirements as defined in the accreditation preliminary recommendation. Should the Identity Provider be found in breach of the accreditation policy and requirements, it will be given an opportunity to cure the breach, but in cases of repeated non-compliance or audit failure, a new Identity Provider must be identified.

Any audit of an Identity Provider shall be tailored for the purpose of assessing compliance, and the auditor MUST give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data and other information requested.

As part of such audits, the Identity Provider shall provide to the auditor in a timely manner all responsive documents, data, and any other information necessary to demonstrate its compliance with the accreditation policy.

Audits of Accredited Entities/Individuals

Appropriate mechanisms must be developed in the implementation phase to ensure accredited entities' and individuals' compliance with the policy requirements as defined in the accreditation preliminary recommendation. These could include, for example, audits triggered by complaints, random audits, or audits in response to a self-certification or self-assessment. Should the accredited entity or individual be found in breach of the accreditation policy and requirements, it will be given an opportunity to cure the breach, but in cases of repeated non-compliance or audit failure the matter should be referred back to the Accreditation Authority for action.

Any audit of accredited entities/individuals shall be tailored for the purpose of assessing compliance, and the auditor MUST give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data and other information requested.

As part of such audits, the accredited entity/individual shall, in a timely manner, provide to the auditor all responsive documents, data, and any other information necessary to demonstrate its compliance with the accreditation policy.

Audits of Entity disclosing the data / Contracted Parties

The EPDP Team will further consider these requirements once the EPDP Team has decided on the roles and responsibilities of the different parties in the SSAD.

NOTE: Depending on the ultimate SSAD model the EPDP Team recommends, there may be other relevant parties that would be subject to auditing. This will be revisited when the ultimate SSAD model is recommended.

SSAD Implementation Guidance

Implementation Guidance #i.
The EPDP Team recommends that, consistent with the preliminary recommendation that an SSAD request 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.

5 Next Steps

5.1 Next Steps

The EPDP Team will complete the next phase of its work and develop its recommendations in a Final Report to be sent to the GNSO Council for review following its analysis of public comments received on this Initial Report. If adopted by the GNSO Council, the Final Report would then be forwarded to the ICANN Board of Directors for its consideration and, potentially, approval as an ICANN Consensus Policy.

Glossary

1. Advisory Committee
An Advisory Committee is a formal advisory body made up of representatives from the Internet community to advise ICANN on a particular issue or policy area. Several are mandated by the ICANN Bylaws and others may be created as needed. Advisory committees have no legal authority to act for ICANN, but report their findings and make recommendations to the ICANN Board.

2. ALAC - At-Large Advisory Committee
ICANN's At-Large Advisory Committee (ALAC) is responsible for considering and providing advice on the activities of the ICANN, as they relate to the interests of individual Internet users (the "At-Large" community). ICANN, as a private sector, non-profit corporation with technical management responsibilities for the Internet's domain name and address system, will rely on the ALAC and its supporting infrastructure to involve and represent in ICANN a broad set of individual user interests.

3. Business Constituency
The Business Constituency represents commercial users of the Internet. The Business Constituency is one of the Constituencies within the Commercial Stakeholder Group (CSG) referred to in Article 11.5 of the ICANN bylaws. The BC is one of the stakeholder groups and constituencies of the Generic Names Supporting Organization (GNSO) charged with the responsibility of advising the ICANN Board on policy issues relating to the management of the domain name system.

4. ccNSO - The Country-Code Names Supporting Organization
The ccNSO the Supporting Organization responsible for developing and recommending to ICANN's Board global policies relating to country code top-level domains. It provides a forum for country code top-level domain managers to meet and discuss issues of concern from a global perspective. The ccNSO selects one person to serve on the board.

5. ccTLD - Country Code Top Level Domain
ccTLDs are two-letter domains, such as .UK (United Kingdom), .DE (Germany) and .JP (Japan) (for example), are called country code top level domains (ccTLDs) and correspond to a country, territory, or other geographic location. The rules and policies for registering domain names in the ccTLDs vary significantly and ccTLD registries limit use of the ccTLD to citizens of the corresponding country.

For more information regarding ccTLDs, including a complete database of designated ccTLDs and managers, please refer to http://www.iana.org/cctld/cctld.htm.

6. Domain Name Registration Data
Domain name registration data, also referred to registration data, refers to the information that registrants provide when registering a domain name and that registrars or registries collect. Some of this information is made available to the public. For interactions between ICANN Accredited Generic Top-Level Domain (gTLD) registrars and registrants, the data elements are specified in the current RAA. For country code Top Level Domains (ccTLDs), the operators of these TLDs set their own or follow their government's policy regarding the request and display of registration information.

7. Domain Name
As part of the Domain Name System, domain names identify Internet Protocol resources, such as an Internet website.

8. DNS - Domain Name System
DNS refers to the Internet domain-name system. The Domain Name System (DNS) helps users to find their way around the Internet. Every computer on the Internet has a unique address - just like a telephone number - which is a rather complicated string of numbers. It is called its "IP address" (IP stands for "Internet Protocol"). IP Addresses are hard to remember. The DNS makes using the Internet easier by allowing a familiar string of letters (the "domain name") to be used instead of the arcane IP address. So instead of typing 207.151.159.3, you can type www.internic.net. It is a "mnemonic" device that makes addresses easier to remember.

9. EPDP – Expedited Policy Development Process
A set of formal steps, as defined in the ICANN bylaws, to guide the initiation, internal and external review, timing and approval of policies needed to coordinate the global Internet's system of unique identifiers. An EPDP may be initiated by the GNSO Council only in the following specific circumstances: (1) to address a narrowly defined policy issue that was identified and scoped after either the adoption of a GNSO policy recommendation by the ICANN Board or the implementation of such an adopted recommendation; or (2) to provide new or additional policy recommendations on a specific policy issue that had been substantially scoped previously, such that extensive, pertinent background information already exists, e.g. (a) in an Issue Report for a possible PDP that was not initiated; (b) as part of a previous PDP that was not completed; or (c) through other projects such as a GNSO Guidance Process.

10. GAC - Governmental Advisory Committee
The GAC is an advisory committee comprising appointed representatives of national governments, multi-national governmental organizations and treaty organizations, and distinct economies. Its function is to advise the ICANN Board on matters of concern to governments. The GAC will operate as a forum for the discussion of government interests and concerns, including consumer interests. As an advisory committee, the GAC has no legal authority to act for ICANN, but will report its findings and recommendations to the ICANN Board.

11. General Data Protection Regulation (GDPR)

The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas.

12. GNSO - Generic Names Supporting Organization
The supporting organization responsible for developing and recommending to the ICANN Board substantive policies relating to generic top-level domains. Its members include representatives from gTLD registries, gTLD registrars, intellectual property interests, Internet service providers, businesses and non-commercial interests.

13. Generic Top Level Domain (gTLD)
"gTLD" or "gTLDs" refers to the top-level domain(s) of the DNS delegated by ICANN pursuant to a registry agreement that is in full force and effect, other than any country code TLD (ccTLD) or internationalized domain name (IDN) country code TLD.

14. gTLD Registries Stakeholder Group (RySG)
The gTLD Registries Stakeholder Group (RySG) is a recognized entity within the Generic Names Supporting Organization (GNSO) formed according to Article X, Section 5 (September 2009) of the Internet Corporation for Assigned Names and Numbers (ICANN) Bylaws.

The primary role of the RySG is to represent the interests of gTLD registry operators (or sponsors in the case of sponsored gTLDs) ("Registries") (i) that are currently under contract with ICANN to provide gTLD registry services in support of one or more gTLDs; (ii) who agree to be bound by consensus policies in that contract; and (iii) who voluntarily choose to be members of the RySG. The RySG may include Interest Groups as defined by Article IV. The RySG represents the views of the RySG to the GNSO Council and the ICANN Board of Directors with particular emphasis on ICANN consensus policies that relate to interoperability, technical reliability and stable operation of the Internet or domain name system.

15. ICANN - The Internet Corporation for Assigned Names and Numbers
The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. Originally, the Internet Assigned Numbers Authority (IANA) and other entities performed these services under U.S. Government contract. ICANN now performs the IANA function. As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes.

16. Intellectual Property Constituency (IPC)
The Intellectual Property Constituency (IPC) represents the views and interests of the intellectual property community worldwide at ICANN, with a particular emphasis on trademark,

copyright, and related intellectual property rights and their effect and interaction with Domain Name Systems (DNS). The IPC is one of the constituency groups of the Generic Names Supporting Organization (GNSO) charged with the responsibility of advising the ICANN Board on policy issues relating to the management of the domain name system.

17. Internet Service Provider and Connectivity Provider Constituency (ISPCP)
The ISPs and Connectivity Providers Constituency is a constituency within the GNSO. The Constituency's goal is to fulfill roles and responsibilities that are created by relevant ICANN and GNSO bylaws, rules or policies as ICANN proceeds to conclude its organization activities. The ISPCP ensures that the views of Internet Service Providers and Connectivity Providers contribute toward fulfilling the aims and goals of ICANN.

18. Name Server
A Name Server is a DNS component that stores information about one zone (or more) of the DNS name space.

19. Non Commercial Stakeholder Group (NCSG)
The Non Commercial Stakeholder Group (NCSG) is a Stakeholder Group within the GNSO. The purpose of the Non Commercial Stakeholder Group (NCSG) is to represent, through its elected representatives and its Constituencies, the interests and concerns of noncommercial registrants and noncommercial Internet users of generic Top-level Domains (gTLDs). It provides a voice and representation in ICANN processes to: non-profit organizations that serve noncommercial interests; nonprofit services such as education, philanthropies, consumer protection, community organizing, promotion of the arts, public interest policy advocacy, children's welfare, religion, scientific research, and human rights; public interest software concerns; families or individuals who register domain names for noncommercial personal use; and Internet users who are primarily concerned with the noncommercial, public interest aspects of domain name policy.

20. Post Delegation Dispute Resolution Procedures (PDDRPs)
Post-Delegation Dispute Resolution Procedures have been developed to provide those harmed by a new gTLD Registry Operator's conduct an alternative avenue to complain about that conduct. All such dispute resolution procedures are handled by providers external to ICANN and require that complainants take specific steps to address their issues before filing a formal complaint. An Expert Panel will determine whether a Registry Operator is at fault and recommend remedies to ICANN.

21. Registered Name
"Registered Name" refers to a domain name within the domain of a gTLD, whether consisting of two (2) or more (e.g., john.smith.name) levels, about which a gTLD Registry Operator (or an Affiliate or subcontractor thereof engaged in providing Registry Services) maintains data in a Registry Database, arranges for such maintenance, or derives revenue from such maintenance. A name in a Registry Database may be a Registered Name even though it does not appear in a zone file (e.g., a registered but inactive name).

22. Registrar
The word "registrar," when appearing without an initial capital letter, refers to a person or entity that contracts with Registered Name Holders and with a Registry Operator and collects registration data about the Registered Name Holders and submits registration information for entry in the Registry Database.

23. Registrars Stakeholder Group (RrSG)
The Registrars Stakeholder Group is one of several Stakeholder Groups within the ICANN community and is the representative body of registrars. It is a diverse and active group that works to ensure the interests of registrars and their customers are effectively advanced. We invite you to learn more about accredited domain name registrars and the important roles they fill in the domain name system.

24. Registry Operator
A "Registry Operator" is the person or entity then responsible, in accordance with an agreement between ICANN (or its assignee) and that person or entity (those persons or entities) or, if that agreement is terminated or expires, in accordance with an agreement between the US Government and that person or entity (those persons or entities), for providing Registry Services for a specific gTLD.

25. Registration Data Directory Service (RDDS)
Domain Name Registration Data Directory Service or RDDS refers to the service(s) offered by registries and registrars to provide access to Domain Name Registration Data.

26. Registration Restrictions Dispute Resolution Procedure (RRDRP)
The Registration Restrictions Dispute Resolution Procedure (RRDRP) is intended to address circumstances in which a community-based New gTLD Registry Operator deviates from the registration restrictions outlined in its Registry Agreement.

27. SO - Supporting Organizations
The SOs are the three specialized advisory bodies that advise the ICANN Board of Directors on issues relating to domain names (GNSO and CCNSO) and, IP addresses (ASO).

28. SSAC - Security and Stability Advisory Committee
An advisory committee to the ICANN Board comprised of technical experts from industry and academia as well as operators of Internet root servers, registrars and TLD registries.

29. TLD - Top-level Domain
TLDs are the names at the top of the DNS naming hierarchy. They appear in domain names as the string of letters following the last (rightmost) ".", such as "net" in http://www.example.net. The administrator for a TLD controls what second-level names are recognized in that TLD. The administrators of the "root domain" or "root zone" control what TLDs are recognized by the DNS. Commonly used TLDs include .COM, .NET, .EDU, .JP, .DE, etc.

30. Uniform Dispute Resolution Policy (UDRP)
The Uniform Dispute Resolution Policy (UDRP) is a rights protection mechanism that specifies the procedures and rules that are applied by registrars in connection with disputes that arise over the registration and use of gTLD domain names. The UDRP provides a mandatory administrative procedure primarily to resolve claims of abusive, bad faith domain name registration. It applies only to disputes between registrants and third parties, not disputes between a registrar and its customer.

31. Uniform Rapid Suspension (URS)
The Uniform Rapid Suspension System is a rights protection mechanism that complements the existing Uniform Domain-Name Dispute Resolution Policy (UDRP) by offering a lower-cost, faster path to relief for rights holders experiencing the most clear-cut cases of infringement.

32. WHOIS
WHOIS protocol is an Internet protocol that is used to query databases to obtain information about the registration of a domain name (or IP address). The WHOIS protocol was originally specified in RFC 954, published in 1985. The current specification is documented in RFC 3912. ICANN's gTLD agreements require registries and registrars to offer an interactive web page and a port 43 WHOIS service providing free public access to data on registered names. Such data is commonly referred to as "WHOIS data," and includes elements such as the domain registration creation and expiration dates, nameservers, and contact information for the registrant and designated administrative and technical contacts.

WHOIS services are typically used to identify domain holders for business purposes and to identify parties who are able to correct technical problems associated with the registered domain.

Annex A – System for Standardized Access/Disclosure to Non-public Registration Data – Background Info

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?

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 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.[18]
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

[18] Several noted that this question might not be in scope for the EPDP Team to address.

○ 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 policy recommendations for sharing of non-public Registration Data[19] with requesting parties (System for Standardized Access/Disclosure of Non-Public Registration Data).

Until legal assurances satisfactory to relevant parties are provided, the development of the

[19] From the EPDP Phase 1 Final Report: "Registration Data" will mean the data elements identified in Annex D [of the EPDP Phase 1 Final Report], collected from a natural and legal person in connection with a domain name registration.

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:

- Terminology and Working Definitions
- Legal guidance needed
- Requirements, incl. defining user groups, criteria & criteria/content of request
- Publication of process, criteria and content request required
- Timeline of process
- Receipt of acknowledgment
- Accreditation
- Authentication & Authorization
- Purposes for third party disclosure
- Lawful basis for disclosure
- Acceptable Use Policy
- Terms of use / disclosure agreements, including fulfillment of legal requirements
- Privacy policies
- Query policy
- 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 / authorization / accreditation of user groups
↓
e) Criteria/content of requests per user group

↓

f) Query policy

↓

g) Receipt of acknowledgement, including timeline

↓

h) Response requirements / expectations, including timeline/SLAs

↓

i) Acceptable Use Policy

↓

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 and other worksheets, 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.

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
1. There is a need to confirm that disclosure for legitimate purposes is not incompatible with the purposes for which such data has been collected.	**ON HOLD** The Phase 2 LC has noted this question as premature at this time and will mark the question as "on hold". The question will be revisited once the EPDP Team has identified the purposes for disclosure.	
2. 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 (IPC)	**REWORK** The Phase 2 LC is in the process of rewording this question, and, upon review of the updated text, will determine if the question should be forwarded to outside counsel.	
3. Legal guidance should be sought on the possibility of an accreditation-based disclosure system as such. (ISPCP)	**ON HOLD** The Phase 2 LC has noted this question as premature at this time and will mark the question as "on	

	hold". The question will be revisited once the EPDP Team has identified the purposes for disclosure.	
4. The question of disclosure to non-EU law enforcement based on Art 6 I f GDPR should be presented to legal counsel. (ISPCP)	**REWORK** The Phase 2 LC is in the process of seeking further guidance from the author of this question, and, upon review of the guidance and/or updated text, will determine if the question should be forwarded to outside counsel.	
5. 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 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? (ISPCP)	**REWORK** The Phase 2 LC is in the process of rewording this question, and, upon review of the updated text, will determine if the question should be forwarded to outside counsel.	

6. Within the context of an SSAD, in addition to determining its own lawful basis for disclosing data, does the requestee (entity that houses the requested data) need to assess the lawful basis of the third party requestor? (Question from ICANN65 from GAC/IPC)	**REWORK** The Phase 2 LC is in the process of rewording this question, and, upon review of the updated text, will determine if the question should be forwarded to outside counsel.	
7. To what extent, if any, are contracted parties accountable when a third party misrepresents their intended processing, and how can this accountability be reduced? (BC)	**REWORK** The Phase 2 LC is in the process of rewording this question, and, upon review of the updated text, will determine if the question should be forwarded to outside counsel.	
8. BC Proposes that the EPDP split Purpose 2 into two separate purposes: ● Enabling ICANN to maintain the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission and Bylaws though the controlling and processing of gTLD registration data. ● Enabling third parties to address consumer protection, cybersecurity, intellectual property, cybercrime, and DNS abuse involving the use or registration of domain names. counsel be consulted to determine if the restated purpose 2 (as stated above) Can legal counsel be consulted to determine if the restated purpose 2 (as stated above) is possible under GDPR? If the above language is not possible, are there suggestions that	**ON HOLD** The Phase 2 LC has noted this question as premature at this time and will mark the question as "on hold". The question will be revisited once the GNSO Council and Board consultations re: Recommendation 1, Purpose 2 have been completed.	

counsel can make to improve this language? (BC)		
9. Can legal analysis be provided on how the balancing test under 6(1)(f) is to be conducted, and under which circumstances 6(1)(f) might require a manual review of a request? (BC)	**REWORK** The Phase 2 LC is in the process of rewording this question, and, upon review of the updated text, will determine if the question should be forwarded to outside counsel.	
10. If not all requests benefit from manual review, is there a legal methodology to define categories of requests (e.g. rapid response to a malware attack or contacting a non-responsive IP infringer) which can be structured to reduce the need for manual review? (BC)	**REWORK** The Phase 2 LC is in the process of rewording this question, and, upon review of the updated text, will determine if the question should be forwarded to outside counsel.	
11. Can legal counsel be consulted to determine whether GDPR prevents higher volume access for properly credentialed cybersecurity professionals, who have agreed on appropriate safeguards? If such access is not prohibited, can counsel provide examples of safeguards (such as pseudonymization) that should be considered? (BC)	**REWORK** The Phase 2 LC is in the process of rewording this question, and, upon review of the updated text, will determine if the question should be forwarded to outside counsel.	
12. To identify 6(1)(b) as purpose for processing registration data, we should follow up on the B & B advice that- “it will be	**REWORK**	

necessary to require that the specific third party or at least the processing by the third party is, at least abstractly, already known to the data subject at the time the contract is concluded and that the controller, as the contractual partner, informs the data subject of this prior to the transfer to the third party" B&B should clarify why it believes that the only basis for providing WHOIS is for the prevention of DNS abuse. Its conclusion in Paragraph 10 does not consider the other purposes identified by the EPDP in Rec 1, and, in any event should consider the recent EC recognition that ICANN has a broad purpose to: 'contribute to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission', which is at the core of the role of ICANN as the "guardian" of the Domain Name System."	The Phase 2 LC is in the process of rewording this question, and, upon review of the updated text, will determine if the question should be forwarded to outside counsel.	
13. B&B should advise on the extent to which GDPR's public interest basis 6(1)e is applicable, in light of the EC's recognition that: "With regard to the formulation of purpose two, the European Commission acknowledges ICANN's central role and responsibility for ensuring the security, stability and resilience of the Internet Domain Name System and that in doing so it acts in the public interest."	**REWORK** The Phase 2 LC is in the process of rewording this question, and, upon review of the updated text, will determine if the question should be forwarded to outside counsel.	

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.

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").

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 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)

d) Authentication / authorization / accreditation of user groups

Objective:

- Establish if authentication, authorization 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, authorization 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.

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?

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.

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 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) Criteria / content of requests per user group

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

Related mind map questions:

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

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 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

f) Query policy

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?

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.

Materials to review:

○ Description	○ Link	○ Required because
SSAC 101 - SSAC Advisory Regarding Access to Domain Name Registration Data	https://www.icann.org/en/system/files/files/sac-101-en.pdf	Describes effects of rate-limiting.

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?

Related mind map questions:

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

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 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?

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.

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 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

i) Acceptable Use Policy

Objective: Define the policy requirements around:

1. How should a code of conduct (if any) be developed, continuously evolve and be enforced?
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?

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?

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

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?

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

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 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

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.

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 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?

Related mind map questions: None

Materials to review:

○ Description	○ Link	○ Required because

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

Annex B – General Background

Process & Issue Background

On 19 July 2018, the GNSO Council initiated an Expedited Policy Development Process (EPDP) and chartered the EPDP on the Temporary Specification for gTLD Registration Data Team. Unlike other GNSO PDP efforts, which are open for anyone to join, the GNSO Council chose to limit the membership composition of this EPDP, primarily in recognition of the need to complete the work in a relatively short timeframe and to resource the effort responsibly. GNSO Stakeholder Groups, the Governmental Advisory Committee (GAC), the Country Code Supporting Organization (ccNSO), the At-Large Advisory Committee (ALAC), the Root Server System Advisory Committee (RSSAC) and the Security and Stability Advisory Committee (SSAC) were each been invited to appoint up to a set number of members and alternates, as outlined in the charter. In addition, the ICANN Board and ICANN Org have been invited to assign a limited number of liaisons to this effort. A call for volunteers to the aforementioned groups was issued in July, and the EPDP Team held its first phase 1 meeting on 1 August 2018.

○ Issue Background

On 17 May 2018, the ICANN Board approved the Temporary Specification for gTLD Registration Data. The Board took this action to establish temporary requirements for how ICANN and its contracted parties would continue to comply with existing ICANN contractual requirements and community-developed policies relate to WHOIS, while also complying with the European Union (EU)'s General Data Protection Regulation (GDPR). The Temporary Specification has been adopted under the procedure for Temporary Policies outlined in the Registry Agreement (RA) and Registrar Accreditation Agreement (RAA). Following adoption of the Temporary Specification, the Board "shall immediately implement the Consensus Policy development process set forth in ICANN's Bylaws".[20] This Consensus Policy development process on the Temporary Specification would need to be carried out within a one-year period. Additionally, the scope includes discussion of a standardized access system to nonpublic registration data.

At its meeting on 19 July 2018, the Generic Names Supporting Organization (GNSO) Council initiated an EPDP on the Temporary Specification for gTLD Registration Data and adopted the EPDP Team charter. Unlike other GNSO PDP efforts, which are open for anyone to join, the GNSO Council chose to limit the membership composition of this EPDP, primarily in recognition of the need to complete the work in a relatively short timeframe and to resource the effort responsibly. GNSO Stakeholder Groups, the Governmental Advisory Committee (GAC), the Country Code Supporting Organization (ccNSO), the At-Large Advisory Committee (ALAC), the Root Server System Advisory Committee (RSSAC) and the Security and Stability Advisory Committee (SSAC) were each been invited to appoint up to a set number of members and

[20] See section 3.1(a) of the Registry Agreement: https://www.icann.org/resources/unthemed-pages/org-agmt-html-2013-09-12-en

alternates, as outlined in the charter. In addition, the ICANN Board and ICANN Org have been invited to assign a limited number of liaisons to this effort.

The EPDP Team published its Phase 1 Initial Report for Public Comment on 21 November 2018. The EPDP Team incorporated public comments into its Phase 1 Final Report, and the GNSO Council voted to adopt all 29 recommendations within the EPDP's Phase 1 Final Report at its meeting on 4 March 2019. On 15 May 2019, the ICANN Board adopted the EPDP Team's Phase 1 Final Report, with the exception of parts of two recommendations: 1) Purpose 2 in Recommendation 1 and 2) the option to delete data in the Organization field in Recommendation 12. As per the ICANN Bylaws, a consultation will take place between the GNSO Council and the ICANN Board to discuss the parts of the EPDP Phase 1 recommendations that were not adopted by the ICANN Board. At the same time, an Implementation Review Team (IRT), consisting of the ICANN organization (ICANN org) and members of the ICANN community, will now implement the approved recommendations of the EPDP Team's Phase 1 Final Report. For further details on the status of implementation, please see here.

On 2 May 2019, the EPDP Team begun Phase 2 of its work. The scope for EPDP Phase 2 includes (i) discussion of a system for standardized access/disclosure to nonpublic registration data, (ii) issues noted in the Annex to the Temporary Specification for gTLD Registration Data ("Important Issues for Further Community Action"), and (iii) issues deferred from Phase 1, e.g., legal vs natural persons, redaction of city field, et. al. For further details, please see here.

Annex C – EPDP Team Membership and Attendance

EPDP Team Membership and Attendance

The members of the EPDP Team are:

	Members / Liaisons[21]	Affiliation	SOI	% of Meetings Attended[22]
1	Alan Woods	RySG	SOI	
2	Matthew Crossman	RySG	SOI	
3	Marc Anderson	RySG	SOI	
4	James M. Bladel	RrSG	SOI	
5	Matt Serlin	RrSG	SOI	
6	Volker Greimann	RrSG	SOI	
7	Alex Deacon	IPC	SOI	
8	Brian King	IPC	SOI	
9	Margie Milam	BC	SOI	
10	Mark Svancarek	BC	SOI	
11	Fiona Assonga	ISPCP	SOI	
12	Thomas Rickert	ISPCP	SOI	
13	Stephanie Perrin	NCSG	SOI	
14	Ayden Férdeline	NCSG	SOI	
15	Milton Mueller	NCSG	SOI	
16	Julf Helsingius	NCSG	SOI	
17	Amr Elsadr	NCSG	SOI	
18	Farzaneh Badiei	NCSG	SOI	

[21] For historic data on members / alternates, please see https://community.icann.org/x/3JUzBw.
[22] This does not include attendance to F2F meetings which is recorded separately. See [to be updated].

19	Georgios Tselentis	GAC	SOI	
20	Chris Lewis-Evans	GAC	SOI	
21	Laureen Kapin	GAC	SOI	
22	Alan Greenberg	ALAC	SOI	
23	Hadia Elminiawi	ALAC	SOI	
24	Greg Aaron	SSAC	SOI	
25	Ben Butler	SSAC	SOI	
26	Chris Disspain	ICANN Board Liaison	SOI	
27	Becky Burr	ICANN Board Liaison	SOI	
28	Rafik Dammak	GNSO Council Liaison	SOI	
29	Eleeza Agopian	ICANN Org Liaison (MSSI)	n/a	
30	Dan Halloran	ICANN Org Liaison (Legal)	n/a	
31	Janis Karklins	EPDP Team Chair	SOI	

The alternates of the EPDP Team are:

	Alternate	Affiliation	SOI	% of Meetings Attended
1	Beth Bacon	RySG	SOI	
2	Arnaud Wittersheim	RySG	SOI	
3	Sean Baseri	RySG	SOI	
4	Owen Smigelski	RrSG	SOI	
5	Sarah Wyld	RrSG	SOI	
6	Theo Geurts	RrSG	SOI	
7	Jennifer Gore	IPC	SOI	
8	Steve DelBianco	BC	SOI	
9	Suman Lal Pradhan	ISPCP	SOI	

10	Tatiana Tropina	NCSG	SOI	
11	David Cake	NCSG	SOI	
12	Stefan Filipovic	NCSG	SOI	
13	Olga Cavalli	GAC	SOI	
14	Rahul Gosain	GAC	SOI	
15	TBD	GAC		
16	Holly Raiche	ALAC	SOI	
17	Bastiaan Goslings	ALAC	SOI	
18	Tara Whalen	SSAC	SOI	
19	Rod Rasmussen	SSAC	SOI	

The detailed attendance records can be found at https://community.icann.org/x/4opHBQ.

The EPDP Team email archives can be found at https://mm.icann.org/pipermail/gnso-epdp-team/.

* The following are the ICANN SO/ACs and GNSO Stakeholder Groups and Constituencies for which EPDP TEAM members provided affiliations:
RrSG – Registrar Stakeholder Group
RySG – Registry Stakeholder Group
BC – Business Constituency
NCSG – Non-Commercial Stakeholder Group
IPC – Intellectual Property Constituency
ISPCP – Internet Service and Connection Providers Constituency
GAC – Governmental Advisory Committee
ALAC – At-Large Advisory Committee
SSAC – Security and Stability Advisory Committee

Annex D - Community Input

Request for Input

According to the GNSO's PDP Manual, an EPDP Team should formally solicit statements from each GNSO Stakeholder Group and Constituency at an early stage of its deliberations. An EPDP Team is also encouraged to seek the opinion of other ICANN Supporting Organizations and Advisory Committees who may have expertise, experience or an interest in the issue. As a result, the EPDP Team reached out to all ICANN Supporting Organizations and Advisory Committees as well as GNSO Stakeholder Groups and Constituencies with a request for input at the start of its deliberations on phase 2. In response, statements were received from:

- The GNSO Business Constituency (BC)
- The GNSO Non-Commercial Stakeholder Group (NCSG)
- The Registries Stakeholder Group (RySG)
- The Registrar Stakeholder Group (RrSG)
- The Internet Service Providers and Connectivity Providers Constituency (ISPCP)

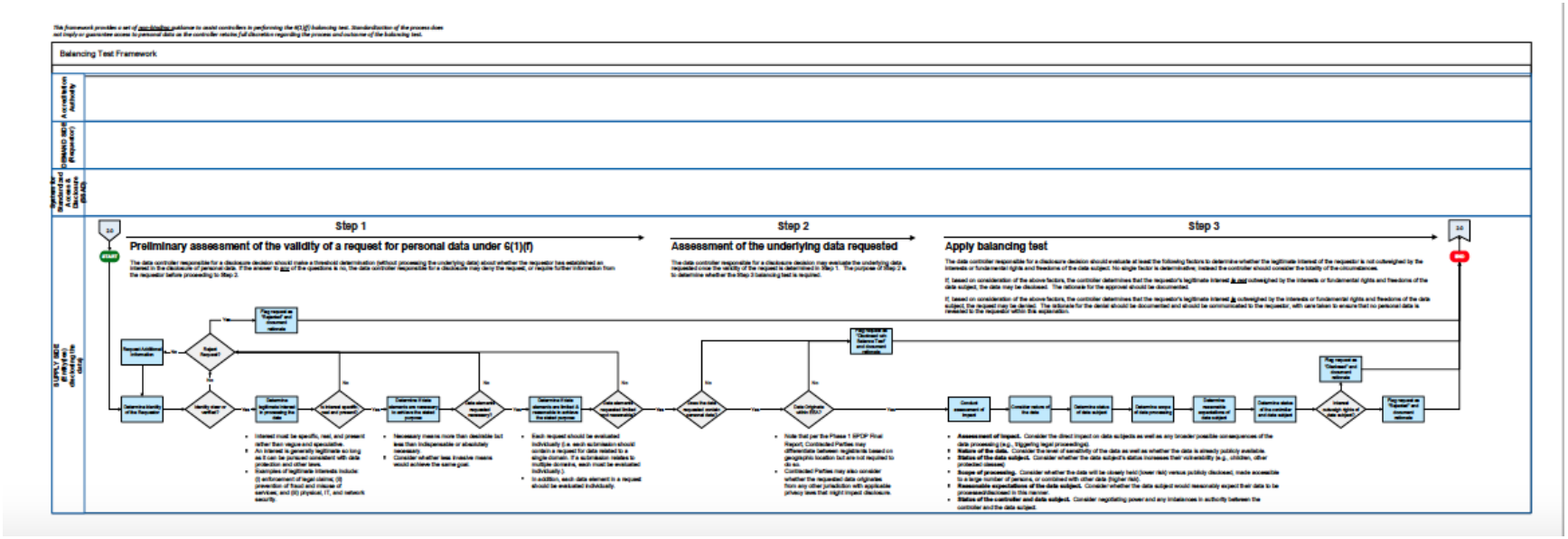
The full statements can be found here: https://community.icann.org/x/zIWGBg.

Review of Input Received

All of the input received was added to the Early Input review tool and considered by the EPDP Team.

Annex E - Balancing Test Framework

See here for standalone file



Annex F – Legal Committee

Phase 2 Questions Submitted to Bird & Bird

1. Consider a System for Standardized Access/Disclosure where:

    - contracted parties "CPs" are contractually required by ICANN to disclose registration data including personal data,
    - data must be disclosed over RDAP to requestors either directly or through an intermediary request accreditation/authorization body,
    - the accreditation is carried out by third party commissioned by ICANN without CP involvement,
    - disclosure takes place in an automated fashion without any manual intervention,
    - data subjects are being duly informed according to ICANN's contractual requirements of the purposes for which, and types of entities by which, personal data may be processed. CP's contract with ICANN also requires CP to notify data subject about this potential disclosure and third-party processing before the data subject enters into the registration agreement with the CP, and again annually via the ICANN-required registration data accuracy reminder. CP has done so.

    Further, assume the following safeguards are in place

    - ICANN or its designee has validated/verified the requestor's identity, and required in each instance that the requestor:
        - represents that it has a lawful basis for requesting and processing the data,
        - provides its lawful basis,
        - represents that it is requesting only the data necessary for its purpose,
        - agrees to process the data in accordance with GDPR, and
        - agrees to EU standard contractual clauses for the data transfer.

    - ICANN or its designee logs requests for non-public registration data, regularly audits these logs, takes compliance action against suspected abuse, and makes these logs available upon request by the data subject.

    1. What risk or liability, if any, would the CP face for the processing activity of disclosure in this context, including the risk of a third party abusing or circumventing the safeguards?

EPDP Phase 2 Legal Committee Summary of Bird & Bird Memo 2:
Question 3: Legitimate Interests and Automated Submissions and/or Disclosures

2. Would you deem the criteria and safeguards outlined above sufficient to make disclosure of registration data compliant? If any risk exists, what improved or additional safeguards would eliminate[1] this risk?

3. In this scenario, would the CP be a controller or a processor[2], and to what extent, if at all, is the CP's liability impacted by this controller/processor distinction?

4. Only answer if a risk still exists for the CP: If a risk still exists for the CP, what additional safeguards might be required to eliminate CP liability depending on the nature of the disclosure request, i.e. depending on whether data is requested e.g. by private actors pursuing civil claims or law enforcement authorities depending on their jurisdiction or the nature of the crime (misdemeanor or felony) or the associated sanctions (fine, imprisonment or capital punishment)?

Footnote 1: "Here it is important to highlight the special role that safeguards may play in reducing the undue impact on the data subjects, and thereby changing the balance of rights and interests to the extent that the data controller's legitimate interests will not be overridden." (https://iapp.org/media/pdf/resource_center/wp217_legitimate-interests_04-2014.pdf)

Footnote 2: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

2. To what extent, if any, are contracted parties liable when a third party that accesses non-public WHOIS data under an accreditation scheme where by the accessor is accredited for the stated purpose, commits to certain reasonable safeguards similar to a code of conduct regarding use of the data, but misrepresents their intended purposes for processing such data, and subsequently processes it in a manner inconsistent with the stated purpose. Under such circumstances, if there is possibility of liability to contracted parties, are there steps that can be taken to mitigate or reduce the risk of liability to the contracted parties?

3. Assuming that there is a policy that allows accredited parties to access non-public WHOIS data through an SSAD (and requires the accredited party to commit to certain reasonable safeguards similar to a code of conduct), is it legally permissible under Article 6(1)(f) to:

- define specific categories of requests from accredited parties (e.g. rapid response to a malware attack or contacting a non-responsive IP infringer), for which there can be automated submissions for non-public WHOIS data, without having to manually verify the qualifications of the accredited parties for each individual disclosure request, and/or
- enable automated disclosures of such data, without requiring a manual review by the controller or processor of each individual disclosure request.

In addition, if it is not possible to automate any of these steps, please provide any guidance for how to perform the balancing test under Article 6(1)(f).

For reference, please refer to the following potential safeguards:

- Disclosure is required under CP's contract with ICANN (resulting from Phase 2 EPDP policy).
- CP's contract with ICANN requires CP to notify the data subject of the purposes for which, and types of entities by which, personal data may be processed. CP is required to notify data subject of this with the opportunity to opt out before the data subject enters into the registration agreement with the CP, and again annually via the ICANN-required registration data accuracy reminder. CP has done so.
- ICANN or its designee has validated the requestor's identity, and required that the requestor:
  - represents that it has a lawful basis for requesting and processing the data,
  - provides its lawful basis,
  - represents that it is requesting only the data necessary for its purpose,
  - agrees to process the data in accordance with GDPR, and
  - agrees to standard contractual clauses for the data transfer.
- ICANN or its designee logs requests for non-public registration data, regularly audits these logs, takes compliance action against suspected abuse, and makes these logs available upon request by the data subject.

4. Under the GDPR, a data controller can disclose personal data to law enforcement of competent authority under Art. 6 1 c GDPR provided the law enforcement authority has the legal authority to create a legal obligation under applicable law. Certain commentators have interpreted "legal obligation" to apply only to legal obligations grounded in EU or Member State law.

As to the data controller:

a. Consequently, does it follow that the data controller may not rely on Art. 6 1 c GDPR to disclose personal data to law enforcement authorities outside the data controller's jurisdiction? Alternatively, are there any circumstances in which data controllers could rely on Art. 6 1 c GDPR to disclose personal data to law enforcement authorities outside the data controller's jurisdiction?

b. May the data controller rely on any other legal bases, besides Art. 6 I f GDPR, to disclose personal data to law enforcement authorities outside the data controller's jurisdiction?

As to the law enforcement authority:

Given that Art. 6 1 GDPR states that European public authorities cannot use Art. 6 I f GDPR as a legal basis for processing carried out in the performance of their tasks, these public authorities need to have a legal basis so that disclosure can take place based on another legal basis (e.g. Art. 6 I c GDPR).

c. In the light of this, is it possible for non-EU-based law enforcement authorities to rely on Art. 6 I f GDPR as a legal basis for their processing? In this context, can the data controller rely on Art. 6 1 f GDPR to disclose the personal data? If non-EU-based law enforcement authorities cannot rely on Art. 6 1 f GDPR as a legal basis for their processing, on what lawful basis can non-EU-based law enforcement rely?

- Executive Summaries[23]

Questions 1 and 2

Executive Summary:
The EPDP Phase 2 team sent its first batch of questions to Bird & Bird on 29 August 2019. Bird & Bird answered this batch of questions in a series of three memos. Memo 1 was delivered on 9 September 2019. Memo 1 analyzed the legal role of contracted parties in the proposed System for Standardized Access/Disclosure (SSAD), the sufficiency of the proposed safeguards, and the risk of liability to contracted parties for disclosure via the SSAD. The questions sent to Bird & Bird are provided in the Annex to this document and include a series of assumptions in Section 1.1 and 1.2 that are part of the factual basis for the responses below.

In response to these questions, Bird & Bird noted the following with respect to controllership:

1. Contracted parties are likely controllers in the SSAD since registrants have traditionally reasonably expected that contracted parties are the controller for disclosure of their data to third parties. It is difficult to show that contracted parties are only serving ICANN org's interests, particularly in light of relevant judicial decisions that suggest a low threshold for controllership.
2. If the EPDP Team wanted to recommend a policy under which contracted parties are processors in a SSAD, steps could be taken to support this policy goal. Contracted parties would need to have no substantial influence over key aspects of SSAD data processing, such as (i) which data shall be processed; (ii) how long shall they be processed; and (iii) who shall have access to the data. There would also be a need for "constant and careful" supervision by ICANN org "to ensure thorough compliance of the processor with instructions and terms of the contract", and efforts to instruct

[23] To be updated when Legal committee signs off on executive summaries

registrants that contracted parties are only acting on ICANN org's behalf (e.g., ICANN org website materials, privacy notices, information in domain name registration process).

3. However, the most likely outcome and starting position for supervisory authorities would be that contracted parties are controllers and likely joint controllers with ICANN org regarding disclosure of registration data through the SSAD.

Bird & Bird noted the following with respect to SSAD safeguards and liability:

4. Given the number of jurisdictions involved, and the likely variety of requests that could be handled by the SSAD, Bird & Bird could not confirm that the criteria and safeguards described in the assumptions would make disclosure of data in a fully automated SSAD compliant.
5. Bird & Bird suggested additional safeguards that the EPDP should consider related to (i) legal basis, proportionality, and data minimization; (ii) individual rights; (iii) international data transfer; and (iv) security.
6. Under the GDPR, parties involved in the same processing are subject to liability to both individuals and supervisory authorities. Individual liability is joint and several, meaning each party involved in the processing is potentially liable for all damages to the data subject, with some differing standards for controllers vs. processors. Supervisory authorities may proceed against controllers or processors, and it is currently unclear whether joint and several liability applies when multiple parties involved in the same processing (i.e., enforcement action isn't appropriate if others are responsible).

---

1. Are Contracted Parties Controllers or Processors?

Controllers

- Liability is significantly impacted by whether Contracted Parties are controllers or processors. (1.4)
- A controller is the "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." (2.2)
- Whether an entity is a controller is a factual determination based on "control over key data processing decisions." The role of controller cannot be assigned or disclaimed. (2.3)
- The Article 29 Working Party provided pre-GDPR guidance on the roles of controller and processor. The EDPB is currently revising this guidance with an update anticipated in the next six months. (2.4, 2.19)

- The EDPB's predecessor, the Article 29 Working Party (WP29) determined that "the first and foremost role of the concept of controller is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice. In other words: to allocate responsibility." Read literally, this reflects that a controller has responsibility for most obligations under the GDPR; but the phrase also indicates a degree of regulatory expediency: it shows the underlying need to hold someone accountable. This can influence a court or supervisory authority's approach, says B&B. (2.4)

- An entity that makes key decisions (alone, or jointly with others) about (i) what data is processed; (ii) the duration of processing; and (iii) who has access to data is acting as a controller, not a processor – these are sometimes referred to as the "essential elements" of processing. (2.6)

- An entity can be both a controller and a processor. This will be the case where an entity that acts as a processor also makes use of personal data for its own purposes. (2.7)

Processors

- A processor is the "natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller." (2.5)

- The Article 29 Working Party guidance emphasizes the importance of examining "'the degree of actual control exercised by a party, the image given to data subjects and the reasonable expectations of data subjects on the basis of this visibility" in determining whether an entity is a controller or processor. (2.5)
- According to WP29, a processor serves "someone else's interest" by "implement[ing] the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means." (2.5)

- A processor can only process personal data pursuant to instructions of the controller or as required by EEA or Member State law. (2.7)

Application to the SSAD

Presumption of controllership

- In some cases, "existing traditional roles that normally imply a certain responsibility will help identifying the controller: for example, the employer in relation to data on his employees, the publisher in relation to data on subscribers, the association in relation to data on its members or contributors". The relation between a Contracted Party and registrant (or registrant's contact) could be regarded in a similar way. (2.8) Similarly, the "image given to data subjects and the reasonable expectations of data subjects" is an important consideration for determining controllership. A registrant will typically

expect that Contracted Parties are the controller for disclosure of their data to third parties. (2.9)

- Since Contracted Parties are currently seen as the controller for disclosure of data to third parties, this will lead to a presumption that Contracted Parties continue to be controllers, even once an SSAD is implemented. (2.9)
- However, such a presumption can't always be made, depending on analysis of technical processing activities. WP169 does note that where there is an assumption that a person is a controller (referred to in WP169 as "control stemming from implicit competence") that this should only be the case "unless other elements indicate the contrary". Recent cases from the CJEU – in particular its recent Fashion ID ruling – have also supported closer, fact-specific analysis. (2.11)

Difficulty presenting Contracted Parties as acting "on behalf of" someone else

- The most important element of a processor's role is that they only act on behalf of the controller. It will be difficult to show that Contracted Parties are only serving ICANN's interests and processing data on ICANN's behalf. (2.10)
- Disclosure of data is likely to be seen as an inevitable consequence of being a Contracted Party, not something that Contracted Parties agree to do on ICANN's behalf. (2.10)

Close factual analysis of technical processing activities

- The factual threshold for becoming a controller (determining purposes or means of processing) is low. The test, according to the CJEU, is simply whether someone "exerts influence over the processing of personal data, for his own purposes, and (…) participates, as a result, in the determination of the purposes and means of that processing". (2.12)
- In the CJEU's Jehovan Todistajat ruling, the national Jehovah's Witnesses community organization was stated to have "general knowledge" and to have encouraged and coordinated data collection by community members (door to door preachers) at a very general level – but it was nevertheless held to have satisfied the test for joint controllership with those community members. In the CJEU's Fashion ID ruling, it was sufficient for the website operator to integrate with Facebook platform code, such that the operator thereby participated in determination of the "means" of Facebook's data collection, and was a joint controller with Facebook. (2.14)
- Courts and supervisory authorities are therefore likely to consider that a Contracted Party is involved in determining the means of processing, possibly just by implementing/interfacing with the SSAD. (2.14)

Factors that could support processor status

- The key to avoid controller status is being able to show that you are not involved in determining the "essential elements" of processing (2.6).
- Also, ICANN monitoring compliance with a contractual requirement to disclose data could be proof of a controller processor relationship, since "constant and careful supervision by the controller to ensure thorough compliance of the processor with instructions and terms of contract provides an indication that the controller is still in full and sole control of the processing operations." (2.16)
- Taking steps to clearly inform data subjects that data is collected only on ICANN's behalf (e.g. disclosures in domain name registration process, annual data accuracy reminder, privacy notices, ICANN org website materials) and other presentations that clearly depict this action as being performed by CPs solely on ICANN's behalf could result in individuals becoming more aware of ICANN's role as a Controller, and the Contracted Parties' role as a processor. (2.17)

Summary – Contracted Parties most likely joint controllers with ICANN

- The most likely outcome and the starting point for supervisory authorities is that Contracted Parties are controllers. (2.18)
- ICANN's role in determining purpose and means of processing suggests they are joint controllers with Contracted Parties for the disclosure of data to third parties. (2.18)

2. Are the Safeguards Proposed Sufficient to Make Disclosure of Registration Data Compliant?

SSAD safeguards

- Given the number of jurisdictions involved, and the likely variety of requests that could be handled by the SSAD, this opinion cannot confirm that the criteria and safeguards described in the assumptions would make disclosure of data in a fully automated system compliant. (3.8)
- B&B states that care must be taken in processing personal data -- a processor (either in breach of its contract with the controller or otherwise behaving in a way inconsistent with the instructions of the controller) can become a controller itself, and thus face breaches (as identified in the table on p.7 of the memo). (3.6)
- The safeguards described are helpful, but will need to include additional measures described below. (3.8)
    - Legal basis: safeguards need to (i) consider whether Contracted Parties, not just Requestor, have a legal basis for processing; (ii) account for the particular legal framework applicable to a Contracted Party; (iii) ensure that an appropriate balancing test is performed on legitimate interests, if that is an appropriate legal

basis in a given case[24] (and it may not be safe to assume that for a category of requests that the balance of interests is always in favor of disclosure; certain cases, such as investigations or prosecutions that could lead to capital punishment, might be especially problematic); and (iv) assurances that improper data types or volumes will not be disclosed to requesters (e.g., rule-based monitoring or blocking of unusual request sizes, permissioning systems). (3.9 – 3.12)

- Individual rights: address how data subject requests are handled, including (i) access rights to request logs (which may themselves be high risk or even "special category" personal data); (ii) appropriate time period for retention of those logs; (iii) the manner in which information is provided to data subjects; (iv) how to deal with situations where Requestor insists on not providing information to the data subject (e.g., law enforcement confidentiality); and (v) requests to restrict or block processing. (3.13 – 3.16)

- Data transfer: for international data transfers, EPDP envisages relying on the EU Standard Contractual Clauses (SCC) legal safeguarding mechanism, however (i) some Requestors, including public authorities, will not agree to their terms; (ii) the terms of the SCCs are not easy to comply with, especially at scale; (iii) if EEA Contracted Parties are processors they cannot directly rely on SCCs to transfer data to ICANN org or Requestors outside of the EEA, so a workaround would need to be found. (3.17)

- Security: safeguards should be proportionate to the risk to data subjects should their data be compromised. (3.18)

3. What is the Risk of Liability to Contracted Parties for Disclosure?

- If the safeguards are inadequate or abused/circumvented by Requestors (or other aspects of the GDPR are contravened, e.g. inadequate notice or lack of a legal basis for processing), Contracted Parties could face investigations, enforcement orders (e.g. processing prohibitions), and (financially) both liability to individuals (civil) and liability to supervisory authorities (fines).

- In broad strokes, B&B offers in pertinent parts that (1) where parties are joint controllers, this does not mean that the parties each have to undertake all elements of compliance, (2) if CPs are processors, they will only be liable to individuals (civil liability) under art. 82 if they have failed to comply with obligations placed on processors under the Regulation, or have acted outside or contrary to lawful instructions from the controller, (3) even when parties are deemed to be joint controllers, recent court decisions (concerning enforcement by supervisory authorities) have emphasized that

[24] If disclosure is a legal obligation pursuant to EU or EU/EEA Member State laws (including treaties to which the EU or a relevant member State is a party), there is no need to consider the legitimate interests test.

joint control does not imply equal responsibility for breaches of the GDPR, and (4) CPs, as joint controllers with ICANN org, would benefit from clear allocation of responsibilities under the terms of the joint controllership "arrangement" they must enter into pursuant to GDPR Art. 26.

Liability to individuals

- GDPR Article 82 sets out the rules on liability to individuals. (4.2)
- Controllers are liable for damages caused by processing that violates GDPR. Processors are liable for damages caused by processing where the processor has not complied with processor specific requirements or where the processor acted outside of or contrary to instructions from the controller. (4.2)
- A controller or processor is not liable if it proves it was in no way responsible for the event resulting in damages. (4.2)
- Where multiple controllers or processors involved in the same processing, each entity is liable for the entire damages (joint and several liability) to individuals (4.2, 4.3)
- If Contracted Parties are processors, they are only liable if they fail to comply with processor-specific obligations under GDPR or act outside or contrary to instructions from the controller. In such a scenario, it is unlikely Contracted Parties would violate the controller's instructions because the SSAD is automated; the more likely source of liability for them, therefore, would be for having inadequate security measures, or failing to comply with the GD{PR's rules on international data transfers. Contracted Parties could look to ICANN org to prescribe security and international transfer arrangements to give Contracted Parties ability to argue that they are "not in any way responsible for the event giving rise to the damage." (4.4)
- If Contracted Parties are controllers, and if disclosure violates GDPR, they are unlikely to avoid liability to individuals if they cannot prove that they are "not in any way responsible for the event giving rise to the damage," if they actively participate in the disclosure event.
- Any liability creates the potential that Contracted Parties would be liable for all damages to the data subject. This risk is highest under a joint controller scenario. (4.5, 4.6).
- Contracted Parties held liable for the entirety of damages to a data subject can seek appropriate contributions from other responsible parties. (4.7)
- As controllers, Contracted Parties and ICANN would have a positive obligation to address the risk of Requestors seeking improper access to personal data. Safeguards must be appropriate to the level of risk. If a Requestor circumvents SSAD safeguards, courts might accept that the safeguards were adequate, which would limit Contracted Parties' primary liability. (4.9, 4.10)

- Even in the event of a GDPR breach caused by a Requestor, the Contracted Parties, ICANN, and the Requestor may be deemed "involved in the same processing" with each party jointly and severally liable for damages arising from that breach. Contracted Parties and ICANN may be able to argue that they are "not in any way responsible for the event giving rise to damage" but otherwise would need to seek recovery from the Requestor or join the Requestor in the initial proceedings in order to apportion damages. (4.11)

  Liability to supervisory authorities

- Supervisory authorities may proceed against controllers or processors. (4.12)

- It is unclear whether joint and several liability applies where multiple parties are involved in processing (i.e., enforcement action arguably isn't appropriate if others are responsible). (4.13)

- There needs to be clear wording in a law, to impose joint and several liability - this strengthens the argument that this would have been stated expressly if it was intended in respect of fines from supervisory authorities. Art. 83(2)(d) makes it clear that joint/several liability doesn't apply concerning supervisory authorities. (4.13.2)
- Even when parties are joint controllers, recent court decisions (about enforcement by supervisory authorities) emphasize that joint control doesn't imply equal responsibility for GDPR breaches. (4.13.4)

- Contracted Parties and ICANN would therefore benefit from clearly allocated responsibilities under a joint controllership arrangement (and a joint controllership arrangement is in any case mandatory, in all joint control siutations, pursuant to GDPR Art. 26). (4.14)

- It may be possible to take advantage of the "lead authority" (a.k.a. "one stop shop" or "consistency") provisions of GDPR to ensure that any enforcement action takes place through ICANN org's Brussels establishment, rather than against Contracted Parties. This mechanism is only available where there is cross-border processing of personal data (entities in multiple EEA member states, or effects on data subjects in multiple EEA member states). (4.15 – 4.17)

- The "lead authority" provisions in GDPR don't specifically address joint controllerships, but guidance suggests that if ICANN org and Contracted Parties designated ICANN's Belgian establishment as the main establishment for the processing (i.e., where decisions regarding processing are made) it may minimize the risk of enforcement directly against Contracted Parties. This is a novel and untested approach. (4.15 – 4.20)

Annex:
Legal Questions 1 & 2: Liability, Safeguards, Controller & Processor

EPDP Phase 2 Legal Committee Summary of Bird & Bird Memo 2:
Question 3: Legitimate Interests and Automated Submissions and/or Disclosures

As the EPDP Team deliberated on the architecture of an SSAD, several questions came up with respect to liability and safeguards. In response, the Phase 2 Legal Committee formulated the following questions to outside counsel:

1. Consider a System for Standardized Access/Disclosure where:

   o contracted parties "CPs" are contractually required by ICANN to disclose registration data including personal data,

   o data must be disclosed over RDAP to requestors either directly or through an intermediary request accreditation/authorization body,

   o the accreditation is carried out by third party commissioned by ICANN without CP involvement,

   o disclosure takes place in an automated fashion without any manual intervention,

   o data subjects are being duly informed according to ICANN's contractual requirements of the purposes for which, and types of entities by which, personal data may be processed. CP's contract with ICANN also requires CP to notify data subject about this potential disclosure and third-party processing before the data subject enters into the registration agreement with the CP, and again annually via the ICANN-required registration data accuracy reminder. CP has done so.

Further, assume the following safeguards are in place

- ICANN or its designee has validated/verified the requestor's identity, and required in each instance that the requestor:
  - represents that it has a lawful basis for requesting and processing the data,
  - provides its lawful basis,
  - represents that it is requesting only the data necessary for its purpose,
  - agrees to process the data in accordance with GDPR, and
  - agrees to EU standard contractual clauses for the data transfer.
- ICANN or its designee logs requests for non-public registration data, regularly audits these logs, takes compliance action against suspected abuse, and makes these logs available upon request by the data subject.

a. What risk or liability, if any, would the CP face for the processing activity of disclosure in this context, including the risk of a third party abusing or circumventing the safeguards?

b. Would you deem the criteria and safeguards outlined above sufficient to make disclosure of registration data compliant? If any risk exists, what improved or additional safeguards would eliminate[25] this risk?

c. In this scenario, would the CP be a controller or a processor[26], and to what extent, if at all, is the CP's liability impacted by this controller/processor distinction?

d. Only answer if a risk still exists for the CP: If a risk still exists for the CP, what additional safeguards might be required to eliminate CP liability depending on the nature of the disclosure request, i.e. depending on whether data is requested e.g. by private actors pursuing civil claims or law enforcement authorities depending on their jurisdiction or the nature of the crime (misdemeanor or felony) or the associated sanctions (fine, imprisonment or capital punishment)?

2. To what extent, if any, are contracted parties liable when a third party that accesses non-public WHOIS data under an accreditation scheme where by the accessor is accredited for the stated purpose, commits to certain reasonable safeguards similar to a code of conduct regarding use of the data, but misrepresents their intended purposes for processing such data, and subsequently processes it in a manner inconsistent with the stated purpose. Under such circumstances, if there is possibility of liability to contracted parties, are there steps that can be taken to mitigate or reduce the risk of liability to the contracted parties?

[25] "Here it is important to highlight the special role that safeguards may play in reducing the undue impact on the data subjects, and thereby changing the balance of rights and interests to the extent that the data controller's legitimate interests will not be overridden." https://iapp.org/media/pdf/resource_center/wp217_legitimate-interests_04-2014.pdf

[26] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

EPDP Phase 2 Legal Committee Summary of Bird & Bird Memo 2:
Question 3: Legitimate Interests and Automated Submissions and/or Disclosures

Question 3

Executive Summary:

The EPDP Phase 2 team sent its first batch of questions to Bird & Bird on 29 August 2019. Bird & Bird answered this batch of questions in a series of three memos. Memo 2 was delivered on 10 September 2019 and analyzed questions related to how the legitimate interests "balancing test" required under GDPR Art 6(1)(f) could be applied in a SSAD, either in highly automated fashion (Question A) or, if it is not possible to automate such a decision, then how the balancing test should be performed (Question B). The full questions are provided in Annex A to this summary and include a series of assumptions that are part of the factual basis for the responses below.

In response to Question A, Bird & Bird noted the following with respect to automation:

1. The highly-automated process described by the EPDP team could amount to solely automated decision making having a legal or similarly significant effect on the data subjects ("data subjects" here would be the targets of requests for nonpublic gTLD data).
2. This is generally is not permitted unless one of the limited legal bases/exemptions under GDPR Art. 22(1) would justify the disclosure. This is much narrower than GDPR Art. 6(1)(f). It would be difficult for the SSAD, as proposed, to meet the GDPR Art. 22(1) exemptions; the SSAD must therefore be structured so it doesn't fall into the scope of Article 22 in the first place.
3. To achieve this it would be necessary to limit automatic access/disclosure to situations where there will be no "legal or similarly significant effects" for the data subject. Examples provided in the memo include the release of admin contact details for non-natural registrants in response to malware attacks or IP infringement. The process for dealing with higher-risk requests should not be fully automated; some meaningful human involvement (at least, oversight) should be present.
4. Alternatively, the SSAD could potentially be structured so that it does not make a decision based on its automatic processing of personal data relating to targets of a request. For example, the SSAD could publish the categories of requests which will be accepted and ask Requestors to confirm that they meet the relevant criteria. By instead requiring *the Requestor* to conduct the necessary analysis and then certify the outcome to the SSAD, the SSAD would then arguably not make a decision (to release data) based on its own automated processing of personal data, so GDPR Art. 22 would not apply. However, relying on self-certification by Requesters perhaps creates scope for abuse of the system by Requesters, which (as previous answers explained) could mean liability for ICANN and the Contracted Parties.
5. As regards authentication of the Requester (as a distinct step from evaluating the grounds or other parameters of a request), Bird & Bird think it would certainly be

possible to automate the process to authenticate the person making the request. It may also be possible to automate other aspects of the request process.

In response to Question B, Bird & Bird:

1. Set out the EU (WP29)'s official guidance on how the Art. 6(1)(f) legitimate interests balancing test should be conducted;
2. Noted that if ICANN and Contracted Parties are joint controllers, they must both establish a legitimate interest in the processing. So far as Contracted Parties are concerned, it is likely that the relevant interest will be that of the third party, the Requester. ICANN, in contrast, may be able to establish its interest in the security, stability and resilience of the domain name system *as well as* the interest of the third party requester; and
3. Provided a high level discussion of safeguards that could be deployed in order to further tip the scales in favour of the processing envisaged as part of the SSAD.

1. Question A

Question A asks whether GDPR Article 6(1)(f) (the "legitimate interests" legal basis for processing) would allow the SSAD to automatically process requests (at least in certain predefined categories), without requiring manual, request-by-request (i) verification that the request meets the relevant criteria for disclosure; and (ii) disclosure of the relevant registration data.

The SSAD could fall within the scope of GDPR Art. 22, rather than purely being concerned with GDPR Art. 6(1)(f)

- GDPR Art. 6(1)(f) permits automated processing *unless* this would amount to "automated individual decision-making" having legal or similarly significant effects for the data subject ("solely automated decision making"), which generally is not permitted unless one of the more limited legal bases/exemptions under GDPR Art. 22(1) would justify the disclosure.

- While GDPR Article 22 states that a data subject has a "right not to be subject to" such a decision, in practice Article 22 has been interpreted by regulators as a general *prohibition* (i.e. there is no need for the data subject to object to such decision-making).

- The process described by the EPDP team could amount to such automated decision-making affecting the target of a request (for instance, when law enforcement wants to bring a prosecution against individuals running unlawful websites).

- If art.22 applies to the processing described by the EPDP, i.e. **if SSAD processing amounts to an automated individual decision having legal or similarly significant effects, it would not be permitted under GDPR Art. 6(1)(f) (the "legitimate interests"**

basis for processing). Art. 22(1) sets out its own, more limited set of grounds on which Art. 22 decision-making can be based.

- B&B advises that **it will be hard for the SSAD to meet the exemptions in Art. 22(1); so therefore, the EPDP should ensure that SSAD processing does not fall within the scope of Art. 22.**

Mitigation strategy 1: avoiding decisions if they might have "legal or similarly significant effects" for individuals whose data is disclosed

- One way to achieve this could be by limiting automatic access and disclosure to situations where there will not be "legal or similarly significant effects" for the data subject.

- A decision to release data via the SSAD would not in itself have a "legal effect" on the data subject. The more relevant test for the SSAD is "similarly significant effects." This means something similar to having legal effect -- something worthy of attention (e.g., significantly affect the circumstances, behavior or choices of the individuals concerned).[27]

- It may be possible to determine categories of requests that don't have a "legal or similarly significant" effect on the individual, like releasing admin contact details for non-natural (company/organizational/institutional) registrants. Other disclosures involving registrant data of a natural person may be much more likely to have a "similarly significant effect." Considerable care would need to be taken over such analysis.

- For decisions more likely to have a "significant effect", human review or oversight would be necessary. "Token" human involvement would not suffice. For the human review element to count, the controller must ensure meaningful oversight by someone who has the authority and competence to change the decision.

Mitigation strategy 2: Avoiding SSAD designs that involve processing of personal data about the target of a request in order to decide whether to comply with the request

- It may also be possible to structure the SSAD so it doesn't involve "a decision based solely on automated processing." GDPR Article 22 requires the decision to be based on processing *of personal data.* If decisions are based on something other than personal data, GDPR Article 22 does not apply.

- Therefore, rather than the SSAD requesting details from requesters (e.g. information about the target of the request, e.g. the registrant, and why their data is required), and

[27] According to official guidance, the following are classic examples of decisions that could be sufficiently significant: (i) decisions that affect someone's financial circumstances; (ii) decisions that affect access to health services; (iii) decisions that deny employment opportunities or put someone at a serious disadvantage; (iv) decisions that affect someone's access to education.

then analyzing that information (automatically) in order to evaluate whether the relevant criteria for release of non-public registration data are met, the SSAD could instead publish the categories of requests which will be accepted, and ask requestors to confirm that they meet the relevant criteria. In this case, the SSAD would not process *personal data* about the target of the request, in order to reach a decision to release the data – so Article 22 would not apply.

- As noted for earlier questions, parties involved in the SSAD have a responsibility to take "appropriate technical and organisational measures" to protect against the risk of misuse of the SSAD system by Requesters.

- Any decision to rely on self-certification, rather than assessing requests, would therefore need to be balanced carefully against these risk mitigation obligations; this would likely narrow the occasions when this self-declaration approach could be used. Bird & Bird notes that under such a scheme, the SSAD could still ask Requesters to provide additional information about the nature of their request *for audit purposes* – but it would not be used to evaluate the request itself (i.e. it would not be used for automated decision-making).

2. Question B

In this question, **the EPDP team asks for guidance on how to perform the balancing test under 6(1)(f) (assuming it's not possible to automate the steps described).**

- Official guidance is that the balancing test should be divided into four steps:

    1. Assess the interest which the processing meets
    2. Consider the impact on the data subject
    3. Undertake a provisional balancing test
    4. Consider the impact of any additional safeguards deployed to prevent any undue impact on the data subject.

1. Assessing the controller's legitimate interest

- 6(1)(f) says you can lawfully process if it is "necessary for the purposes of the legitimate interests pursued by the controller or a third party."

- There are three sub-elements to this: (i) legitimacy; (ii) existence of an interest; and (iii) necessity.

Legitimacy

- It seems that "legitimacy" is not a high test -- WP29 said "an interest can be considered as legitimate as long as the controller can pursue this interest in a way that is in accordance with data protection and other laws."

EPDP Phase 2 Legal Committee Summary of Bird & Bird Memo 2:
Question 3: Legitimate Interests and Automated Submissions and/or Disclosures

Establishing "interest" in the processing

- B&B notes that if ICANN and Contracted Parties are joint controllers, they must both establish a legitimate interest in the processing. So far as Contracted Parties are concerned, it is likely that the relevant interest will be that of the third party, the requester. ICANN, in contrast, may be able to establish its interest in the security, stability and resilience of the domain name system as well the interest of the third party requester.

- "Interest" is not the same as "purpose."

    - "Purpose" is the specific reason why the data is processed

    - "Interest" is the broader stake that a controller may have in the processing, or the benefit the controller derives, or that society might derive from the processing. (This also means that interests could be public or private; for example, in the case of actions to prevent trademark infringement, there could be a private interest for the person whose trademark has been infringed and a wider public interest in preventing a risk of confusion by the public. This factor could usefully be noted in the documentation of the balancing test.)

- Interest must be "real and specific", not "vague and speculative."

- At p.25, WP217 provides a non-exhaustive list of contexts in which legitimate interests may arise, including:

    - "Exercise of the right to freedom of expression or information, including in the media and the Arts"

    - Enforcement of legal claims

    - Prevention of fraud, misuses of services,

    - Physical security, IT and network security

    - Processing for research purposes

- The EPDP suggests that potential SSAD safeguards could include requiring the requester to represent that it has a lawful basis for making the request and that it can "provide its lawful basis". However, where data will be released pursuant to art.6(1)(f), then it would be more helpful for the requester to confirm its *interest* in receiving the personal data.

Necessity

- With regard to necessity, B&B advises the proposed processing (disclosure) must be "necessary" for this interest.

- The CEJU Oesterreichischer Rundfunk case defines this as: *"…the adjective 'necessary'…implies that a 'pressing social need' is involved and that the measure employed is 'proportionate to the legitimate aim pursued'."*
- A UK Court of appeals likewise suggests that necessary means "more than desirable but less than indispensable or absolutely necessary."

- B&B suggests that a relevant factor to consider for necessity could be whether a requester has tried to make contact with the individual in any other ways (although this may be inappropriate in the case of law enforcement requests).
- B&B notes that the SSAD proposes to ask requesters to confirm they are requesting only data that is necessary for their purpose.

2. Assessing the impact on the individual

- B&B says the EDPB suggests a range of factors to be considered when assessing the impact on the individual:
  - ***Assessment of impact.*** Consider the direct impact on data subjects as well as any broader possible consequences of the data processing (e.g., triggering legal proceedings).
  - ***Nature of the data.*** Consider the level of sensitivity of the data as well as whether the data is already publicly available.
  - ***Status of the data subject***. Consider whether the data subject's status increases their vulnerability (e.g., children, other protected classes).
  - ***Scope of processing.*** Consider whether the data will be closely held (lower risk) versus publicly disclosed, made accessible to a large number of persons, or combined with other data (higher risk).
  - ***Reasonable expectations of the data subject***. Consider whether the data subject would reasonably expect their data to be processed/disclosed in this manner.
  - ***Status of the controller and data subject.*** Consider negotiating power and any imbalances in authority between the controller and the data subject.
- It may be possible for the SSAD to take account of these factors, by identifying requests that would pose a high risk for individuals so that those requests receive additional attention.
- A classic risk methodology (looking at severity and likelihood) can be used in assessing risk.

- This is not a purely quantitative exercise; while a request's metrics (e.g. number of data subjects affected) is relevant, it is not determinative – a potentially significant impact on a single data subject should still be considered.

3. Provisional balance

- Once legitimate interests of the controller or third party and those of the individual have been considered, they can be balanced. Ensuring other data protection obligations are met assists with the balancing but is not determinative (e.g., SSAD ensuring standard contractual clauses in place with requesters regarding adequate protection of data is helpful, because it perhaps reduces risk for individuals, but it is not determinative).

4. Additional safeguards

- B&B reports that if it's not clear how the balance should be struck, the controller can consider additional safeguards to reduce the impact of processing on data subjects.
- These include, for example:
    - Transparency
    - Strengthened subject rights to access or port data
    - Unconditional right to opt out
- WP217, pp. 41-42, provides more details on safeguards that can help "tip the scales" in favour of processing (here, in favour of disclosures), in legitimate interests balancing tes

EPDP Phase 2 Legal Committee Summary of Bird & Bird Memo 2:
Question 3: Legitimate Interests and Automated Submissions and/or Disclosures

Annex: Legal Question 3: legitimate interests and automated submissions and/or disclosures

a) Assuming that there is a policy that allows accredited parties to access non-public WHOIS data through a System for Standardized Access/ Disclosure of non-public domain registration data to third parties ("SSAD") (and requires the accredited party to commit to certain reasonable safeguards similar to a code of conduct), is it legally permissible under Article 6(1)(f) to:

- define specific categories of requests from accredited parties (e.g. rapid response to a malware attack or contacting a non-responsive IP infringer), for which there can be automated submissions for non-public WHOIS data, without having to manually verify the qualifications of the accredited parties for each individual disclosure request, and/or

- enable automated disclosures of such data, without requiring a manual review by the controller or processor of each individual disclosure request.

b) In addition, if it is not possible to automate any of these steps, please provide any guidance for how to perform the balancing test under Article 6(1) (f).

For reference, please refer to the following potential safeguards:

- Disclosure is required under CP's contract with ICANN (resulting from Phase 2 EPDP policy).
- CP's contract with ICANN requires CP to notify the data subject of the purposes for which, and types of entities by which, personal data may be processed. CP is required to notify data subject of this with the opportunity to opt out before the data subject enters into the registration agreement with the CP, and again annually via the ICANN- required registration data accuracy reminder. CP has done so.
- ICANN or its designee has validated the requestor's identity, and required that the requestor:
  - represents that it has a lawful basis for requesting and processing the data,
  - provides its lawful basis,
  - represents that it is requesting only the data necessary for its purpose,
  - agrees to process the data in accordance with GDPR, and
  - agrees to standard contractual clauses for the data transfer.
- ICANN or its designee logs requests for non-public registration data, regularly audits these logs, takes compliance action against suspected abuse, and makes these logs available upon request by the data subject.

EPDP Phase 2 Legal Committee Summary of Bird & Bird Memo 2:
Question 3: Legitimate Interests and Automated Submissions and/or Disclosures

Question 4

Executive Summary:

The EPDP Phase 2 team sent its first batch of questions to Bird & Bird on 29 August 2019. Bird & Bird answered this batch of questions in a series of three memos. Memo 3 was delivered on 9 September 2019 and analyzes questions about the legal bases under which personal data contained in gTLD registration data could be disclosed to law enforcement authorities outside the data controller's jurisdiction.

Specifically, the memo responds to the following questions:

- Can a data controller rely on Article 6(1)(c) of the GDPR to disclose personal data to law enforcement authorities outside the data controller's jurisdiction?
- If not, may the data controller rely on any other legal bases, besides Article 6(1)(f) to disclose personal data to law enforcement authorities outside the data controller's jurisdiction?
- Is it possible for non-EU-based law enforcement authorities to rely on art 6(1)(f) GDPR as a legal basis for their processing? In this context, can the data controller rely on art 6(1)(f) GDPR to disclose the personal data? If non-EU-based law enforcement authorities cannot rely on art 6(1)(f) GDPR as a legal basis for their processing, on what lawful basis can non-EU-based law enforcement rely?

Overall, Bird & Bird advised that:

1. To apply Art 6(1)(c) there must be "Union law or Member State law to which the controller is subject" and this ground therefore has limited application where LEA is outside of the controller's jurisdiction.
2. Under the six lawful bases for processing personal data, Articles 6(1)(a) - Consent, 6(1)(b) - Contract, 6(1)(d) - Vital interests of a person, and 6(1)(e) - Public interest or official authority are not likely applicable for LEA requests.
3. Art 6(1)(f) - Legitimate interest, may be an applicable basis for the controller where a non-EU law enforcement authority makes a request to obtain personal data from a controller in the EU.
4. If a LEA is outside the EEA, their legal basis for processing under GDPR is not relevant as they are not subject to GDPR. Organizations disclosing to LEAs outside the EEA will still need a valid basis to do so, which will usually be legitimate interest in ICANN's case.
5. Where the CP is subject to GDPR but is located outside the EEA, they will also be subject to local law. This means that controllers may face a conflict of laws.

EPDP Phase 2 Legal Committee Summary of Bird & Bird Memo 2:
Question 3: Legitimate Interests and Automated Submissions and/or Disclosures

1. Can a data controller rely on Article 6(1)(c) GDPR to disclose personal data to law enforcement authorities outside the data controller's jurisdiction?

- Processing necessary for compliance with a legal obligation to which the controller is subject is only available where the legal obligation is set out in EU or Member State law.
- Where the controller is subject to disclosure obligations which arise from laws in jurisdictions outside the EU, the controller cannot rely on Art 6(1)(c).
- Controller may be subject to a legal obligation under EU or Member State law to disclose personal data to a non-EU law enforcement authority.
- MLATs may cover, but when a request comes in where an MLAT exists, the controller should deny the request and refer to the MLAT. Where no MLAT or other agreement exists, the controller needs to ensure that the disclosure to a third country would not be in breach of local law.

2. May the data controller rely on any other legal bases, besides Article 6(1)(f) GDPR, to disclose personal data to law enforcement authorities outside the data controller's jurisdiction?

- 6(1)(f) and 6(1)(c) may apply but the other five lawful bases for processing personal data likely not.
- Where a non-EU law enforcement authority makes a request to obtain personal data from a controller in the EU, the controller may be able to show a legitimate interest (6(1)(f)) in disclosing the data. The EDPB has also suggested this approach in correspondence to ICANN (e.g. EDPB-85-2018).

3. Is it possible for non-EU-based law enforcement authorities to rely on Article 6(1)(f) GDPR as a legal basis for their processing? In this context, can the data controller rely on Article 6(1)(f) GDPR to disclose the personal data? If non-EU-based law enforcement authorities cannot rely on Article 6(1)(f) GDPR as a legal basis for their processing, on what lawful basis can non-EU-based law enforcement rely?

- As entities of a country, law enforcement authorities are covered by state immunity and therefore non-EU-based law enforcement authorities are not subject to the GDPR.
- Even assuming the GDPR could apply to non-EU-based law enforcement authorities, it seems unlikely that law enforcement authorities outside the EU would consider justifying their processing under the GDPR.
- Non-EU-based law enforcement authorities therefore do not need to assess which GDPR legal basis they rely on for processing the data.

- A controller who transfers data to a LEA outside the EU will nevertheless need to consider how to meet the obligations in Chapter V (transfers of personal data to third countries or international organizations).