ICANN | GNSO

Generic Names Supporting Organization

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

[Date]

Status of This Document

This is the Final Recommendations Report of the GNSO Expedited Policy Development Process (EPDP) Team on the Temporary Specification for gTLD Registration Data Phase 2 for submission to the GNSO Council.

Preamble

The objective of this Final Report is to document the EPDP Team's: (i) deliberations on charter questions, (ii) input received on the EPDP's Phase 2 Initial Report and the EPDP Team's subsequent analysis, (iii) policy recommendations and associated consensus levels, and (iv) implementation guidance, for GNSO Council consideration.

Table of Contents

1 Executive Summary

1.1 Background

On 17 May 2018, the ICANN Board of Directors (ICANN Board) adopted the Temporary Specification for generic top-level domain (gTLD) Registration Data ("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").[1] 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 Organizations 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 Final 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.

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 Purpose for ICANN's Office of the Chief Technology Officer
- Feasibility of unique contacts to have a uniform anonymized email address
- Accuracy and WHOIS Accuracy Reporting System

[1] 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/.

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.

1.2 Initial Report and Addendum to Initial Report

On 7 February 2020, the EPDP Team published its Initial Report for public comment. The Initial Report outlined the core issues discussed in relation to the proposed System for Standardized Access/Disclosure to non-public gTLD registration data ("SSAD") and accompanying preliminary recommendations.

On 26 March 2020, the EPDP Team published an Addendum to the Initial Report for public comment. The Addendum concerns the EPDP Team's preliminary recommendations and/or conclusions on the priority 2 items as listed above.

Following the publication of the Initial Report and the Addendum to the Initial Report, the EPDP Team: (i) continued to seek guidance on legal issues, (ii) carefully reviewed Public Comments received in response to the publication of the Initial Report and Addendum, (iii) continued to review the work-in-progress with the community groups the Team members represent, and (iv) continued its deliberations for the production of this 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. Consensus calls on the recommendations contained in this Final Report, as required by the GNSO Working Group Guidelines, were carried out by the EPDP Team Chair, as described here: [include link].

Recommendations for GNSO Council consideration (see chapter 3 for full text of recommendations):

SSAD Recommendations:

Recommendation #1. **Accreditation**

Recommendation #2. **Accreditation of governmental entities**

Recommendation #3. **Criteria and Content of Requests**

Recommendation #4. **Acknowledgement of receipt**

Recommendation #5. **Response Requirements**

Recommendation #6. **Priority Levels**

Recommendation #7. Requestor Purposes

Recommendation #8. Contracted Party Authorization

Recommendation #9. Automation of SSAD Processing

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

Recommendation #11. SSAD Terms and Conditions

Recommendation #12. Disclosure Requirement

Recommendation #13. Query Policy

Recommendation #14. Financial Sustainability

Recommendation #15. Logging

Recommendation #16. Audits

Recommendation #17. Reporting Requirements

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

Priority 2 recommendations:

Recommendation #19. Display of information of affiliated privacy / proxy providers

Recommendation #20. City Field

Recommendation #21. Data Retention

Recommendation #22. Purpose 2

Priority 2 conclusions:

Conclusion #1. OCTO Purpose

Conclusion #2. Accuracy and WHOIS Accuracy Reporting System

As a result of external dependencies and time constraints, this Final Report does not address all priority 2 items. The EPDP Team will consult with the GNSO Council on how to address the remaining priority 2 items.

1.3 Conclusions and Next Steps

This Final Report will be submitted to the GNSO Council for its consideration and approval.

1.4 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 Final 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.

2 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.

2.1 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 one or more times per week, in addition to email exchanges on its mailing list. Additionally, the EPDP Team held four face-to-face meetings: the first set of face-to-face discussions took place at the ICANN65 Public Meeting in Marrakech, Morocco, two dedicated set of face-to-face meetings, the second and fourth meeting, were held at the ICANN headquarters in Los Angeles (LA) in September 2019 and January 2020, and the third face-to-face discussion 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 D). This template was also used to record input from other ICANN Supporting Organizations and Advisory Committees and can be found in Annex D.

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.

2.2 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").

2.3 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 Purpose for ICANN's Office of the Chief Technology Officer
- Feasibility of unique contacts to have a uniform anonymized email address
- 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.

2.4 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 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 eight 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.

2.5 Charter Questions

In addressing the charter questions,[2] 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, (5) input provided in response to the public comment forums, and (6) input provided by the EPDP Team's legal advisors, Bird & Bird.

[2] Annex A covers in further detail the linkage between each of the topics addressed in the recommendations and the relevant charter questions.

3 EPDP Team Responses to Charter Questions & Recommendations

After reviewing public comments on the Initial Report and the Addendum to the Initial Report, the EPDP Team presents its recommendations for GNSO Council consideration. This Final Report states the level of consensus within the EPDP Team achieved for the different recommendations. [Placeholder for consensus level statement]. In relation to the SSAD related recommendations, the EPDP Team considers these interdependent and as a result, these must be considered as one package by the GNSO Council and subsequently the ICANN Board.

Note: During Phase 1 of the EPDP Team's work, the EPDP Team was tasked with reviewing the Temporary Specification. The Temporary Specification was established as a response to the GDPR.[3] Accordingly, the GDPR is the only law that is specifically referenced in this report. The EPDP team has extensively deliberated whether this Final Report could be drafted in a way that is agnostic to any specific law, but the EPDP Team determined that the report would benefit from explicit references to facilitate the implementation of the Team's recommendations. The GDPR is a regional law covering multiple jurisdictions and - given the strict criteria it contains - compliance with this law has a high probability of being compliant with other national data protection laws. The EPDP team fully endorses ICANN's aspiration to be globally inclusive, and nothing in this report shall overturn the basic principle that contracted parties can and must comply with locally applicable statutory laws and regulations.

3.1 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 recommendations.

As part of its deliberations, the EPDP Team considered various models but agreed to put the following SSAD model forward for public comment. This SSAD model is based on the following high-level principles/concepts:

- The receipt, authentication, and transmission of SSAD requests must be fully automated insofar as it is technically and commercially feasible and legally permissible. Disclosure decisions should be automated only where technically

[3] "This Temporary Specification for gTLD Registration Data (Temporary Specification) establishes temporary requirements to allow ICANN and gTLD registry operators and registrars to continue to comply with existing ICANN contractual requirements and community-developed policies in light of the GDPR."

and commercially feasible and legally permissible. In areas where automation does not meet these criteria, standardization of the disclosure decision process is the baseline objective. Experience gained over time with SSAD disclosure requests and responses must inform further streamlining and standardization of responses.

- In recognition of the need for experience-based adjustments in the function of SSAD, there should be a GNSO Standing Committee, which will monitor the implementation of the SSAD and recommend improvements that could be made. Improvements recommended through this process must not violate the policies established by the EPDP, data protection laws, ICANN Bylaws, or GNSO Procedures and Guidelines.
- Service level agreements (SLAs) need to be put in place and be enforceable, but these may need to be of an evolutionary nature to recognize that there will be a learning curve.
- Responses to disclosure requests, regardless of whether review is conducted manually or an automated responses is triggered, are returned from the relevant Contracted Party directly to the Requestor, but appropriate logging mechanisms must be in place to allow for the SSAD to confirm that SLAs are met and responses are being processed according to the policy (for example, the Central Gateway MUST be notified when disclosure requests are rejected or granted).

The benefits of this model are:

Single location to submit requests

- Reduces time and effort spent by requesters to track down individual points of contact or follow individual procedures
- Ensures that requests are routed directly to the responsible party at each disclosing entity, thereby eliminating the uncertainty that requests are not received or go to someone unqualified to process them
- Allows for clear outreach opportunities to socialize the location and method for requesting non-public registration data
- Requests and responses can be tracked for SLA adherence

Standardized request forms

- Reduces the number of disclosure requests that are denied due to insufficient information
- Increases the efficiency with which disclosing entities can review requests
- Reduces uncertainty for requesters who now have a standard/uniform set of data to provide when submitting disclosure requests.
- Reduces the need for individual set of required information by disclosing parties

Built-in authentication process

- Speeds up the review process for disclosing entities as they will not need to re-verify the Requestor
- External assurance that Requestors have been verified can increase the likelihood and/or speed of disclosure

Standardized review and response process

- Allows creation of a common response format
- Allows creation of rules, guidelines, and best practices disclosing parties can follow in reviewing and responding to requests
- Allows adoption of common response review system
- Allows automation of certain yet-to-be-defined requests by yet-to-be-defined Requestors
- Facilitates automated disclosure decision making in some scenarios
- The logging of requests and responses also allows ICANN Org to audit the actions of disclosing entities, identifying any instances of systemic non-compliance, and take appropriate enforcement action

Main SSAD Roles & Responsibilities:

- Central Gateway Manager – role performed by or overseen by ICANN Org. Responsible for managing intake and routing of SSAD requests that require manual review to responsible Contracted Parties. Responsible for managing and directing requests that are confirmed to be automated to Contracted Parties for release of data, consistent with the criteria established and agreed to in these policy recommendations or based on the recommendation of the GNSO Standing Committee for the review of the implementation of policy recommendations concerning SSAD. Responsible for collecting data on requests, responses, and disclosure decisions taken.
- Accreditation Authority – role performed by or overseen by ICANN Org. 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 Signed Assertions).
- Identity Provider - Responsible for 1) Verifying the identity of a Requestor and managing an Identifier Credential associated with the Requestor, 2) Verifying and managing Signed Assertions associated with the Identifier Credential. For the purpose of the SSAD, the Identity Provider may be the Accreditation Authority itself or the Accreditation Authority may rely on zero or more third parties to perform the Identity Provider services.

- Contracted Parties – Responsible for responding to disclosure requests that do not meet the criteria for an automated response.4
- GNSO Standing Committee for the review of the implementation of policy recommendations concerning SSAD – Committee representative of the ICANN community responsible for evaluating SSAD operational issues emerging as a result of adopted ICANN Consensus Policies and/or their implementation. The GNSO Standing Committee is intended to examine data being produced as a result of SSAD operations, and provide the GNSO Council with recommendations on how best to make operational changes to the SSAD, which are strictly implementation measures, in addition to recommendations based on reviewing the impact of existing Consensus Policies on SSAD operations.

It is the expectation that the different roles and responsibilities will be outlined in detail and confirmed in the applicable agreements.

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

3.2 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".[5]

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

[4] As a default, the Central Gateway Manager will send disclosure requests to Registrars, but that does not preclude the Central Gateway Manager from sending disclosure request so Registries in certain circumstances (see recommendation #5 for further details).

[5] Please note that the model described here is not the same as the SSAD model put forward in this report by the EPDP Team.

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 posed a number of additional clarifying questions to ICANN org, and they can be found, together with the responses here: https://community.icann.org/x/5BdIBg.

The EPDP Team considered this input, the feedback received from the Belgian DPA, and the input received during the public comment period, to make a final determination of the division of roles and responsibilities in the SSAD.

3.3 SSAD Underlying Assumptions

The EPDP Team used the underlying assumptions outlined below to develop its 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 Final Report and the ultimate policy implementers in understanding the intent and underlying assumptions of the EPDP Team in putting forward the SSAD model and related recommendations.

- The objective of the SSAD is to provide a predictable, transparent, efficient, and accountable mechanism for the access/disclosure of non-public registration data.
- The SSAD must be compliant with the GDPR.
- The SSAD must have the ability to adhere to these policy principles and recommendations.
- Given the decisions made by the EPDP team regarding the SSAD model, the working assumption is that ICANN and Contracted Parties will be Joint Controllers. This designation is based on a factual analysis of the policy as is proposed.

3.4 Conventions Used in this Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 148 [RFC2119] [RFC8174].

Note: Noting the EPDP team's choice of model, and pending the specific legal advice as to the responsibility of the parties and the identification as to the controllership of the data, as it applies to the proposed model, the EPDP team notes that certain statements, throughout the recommendations, may require refinement from

mandatory to permissive and vice versa. (e.g., “Shall” to “should”, “MUST” to “MAY”, etc.).

3.5 EPDP Team SSAD Recommendations

3.5.1. Definitions

- **Accreditation** - An administrative action by which the accreditation authority declares that a user is eligible to use 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 Signed Assertions).
- **Accreditation Authority Auditor** – The entity responsible for carrying out the auditing requirements of the Accreditation Authority, as outlined in Recommendation #16 (Audits). The entity could be an independent body or, if ICANN Org ultimately outsources the role of Accreditation Authority to a third party, ICANN Org MAY be the Accreditation Authority Auditor.
- **Authentication** - The process or action of Validating the Identity Credential and Signed Assertions of a Requestor.
- **Authorization** - A process for approving or denying disclosure of non-public registration data.
- **De-accreditation of Accreditation Authority –** An administrative action by which ICANN org revokes the agreement with the accreditation authority, if this function is outsourced to a third party, following which it is no longer approved to operate as the accreditation authority.
- **Eligible government entity**: a government entity (including local government) that has a purpose to access non-public registration data for the exercise of a public policy task within its mandate.
- **“Identity Credential”:** A data object that is a portable representation of the association between an identifier and authenticated 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.
- **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 Signed Assertions associated with the Identifier Credential. For the purpose of the SSAD, the Identity Provider may be the Accreditation Authority itself or the Accreditation Authority may rely on zero or more third parties to perform the Identity Provider services.
- **Requestor –** An accredited user seeking disclosure of domain name registration data through the SSAD

- **Revocation of User Credentials-** The event that occurs when an Identity Provider declares that a previously valid credential has become invalid.
- **"Signed Assertion"**: A data object that is a portable representation of the association between an Identifier Credential and one or more access assertions, and that can be presented for use in Validating those assertions for an entity that attempts such access. Example: [OAuth credential], X.509 attribute certificate. Signed Assertions may be user-specific (e.g. to indicate professional affiliation or affirmation of lawful data handling processes) or request-specific (e.g. indicating the lawful basis for the disclosure request).
- **Validate/validation -** To test, prove or establish the soundness or correctness of a construct. (Example: The Discloser will Validate the Identity Credential and Signed Assertions as part of its Authorization process.)
- **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.

3.5.2. Recommendations

Recommendation #1. Accreditation[6]

1.1 The EPDP Team recommends that the Accreditation Authority establish a policy for accreditation of SSAD users in accordance with the recommendations outlined below.

1.2 The following recommendations MUST be included in 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 (e.g. legal persons) warrants that the individual is acting on the authority of the accredited entity.[7]

c) The accreditation policy defines a single Accreditation Authority, managed by ICANN org, which is responsible for the verification, issuance, and ongoing management of both the Identity Credential and the Signed

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

[7] Implementation guidance: The accredited entity is expected to develop appropriate policies and procedures to ensure appropriate use by an individual of its credentials. Each user must be accredited, but a user acting on behalf of an organization, must have their accreditation tied to its organization's accreditation.

Assertions. The Accreditation Authority MUST develop a privacy policy. 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. The responsibility for the processing of personal data in this latter case shall remain with the Accreditation Authority. If ICANN org chooses to outsource the Accreditation Authority function or parts thereof, ICANN org will remain responsible for overseeing the party(ies) to which the function or parts thereof is/are outsourced. Overseeing MUST include monitoring for and addressing potential abuse by the party(ies) to which the function of parts thereof has been outsourced.

d) The decision to authorize disclosure of registration data, based on validation of the Identity Credential, Signed Assertions, and data as required in the recommendation concerning criteria and content of requests (Recommendation #3), will reside with the Registrar, Registry or the Central Gateway Manager, as applicable.

1.3 Requirements of the Accreditation Authority

a) Verify the Identity of the Requestor: The Accreditation Authority MUST verify the identity of the Requestor, resulting in an Identity Credential.[8]

b) Management of Signed Assertions: The Accreditation Authority MAY verify and manage a set of dynamic assertions/claims associated with and bound to the Identity Credential of the Requestor. This verification, which may be performed by an Identity Provider, results in a Signed Assertion. Signed Assertions[9] convey information such as:

- Assertion as to the purpose(s) of the request
- Assertion as to the legal basis of the request
- Assertion that the user identified by the Identity Credential is affiliated with the relevant organization
- 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

[8] Implementation guidance: ICANN org should use its experience in other areas where verification is involved, such as registrar accreditation, to put forward a proposal for verification of the identity of the Requestor during the implementation phase.

[9] For clarity, Signed Assertions are dynamic and may change based on the request (purpose, legal basis, type, urgency, etc.) compared to an Identifier Credential, which is static and typically does not change. Signed assertions are only used to associate/bind attributes to an identity. These attributes are dynamic per request, but can be vetted and managed up front as part of the Accreditation Process as needed. The Accreditation Authority can establish various assertions for a specific Identifier Credential up front or dynamically create them on a per request basis. How this is determined is to be further worked out in the implementation phase. The Accreditation Authority may store multiple Signed Assertions per Identifier Credential, but the Requestor must invoke the relevant assertions per request. It should not be the objective to attach as many signed assertions as possible to a request.

- 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.

c) Validation of Identity Credentials and Signed Assertion**s**, in addition to the information contained in the request, facilitate the decision 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 where lawful.

d) Define a baseline "code of conduct"[10] that establishes a set of rules that contribute to the proper application of data protection laws - including the GDPR, 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 Authority 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.

e) The Accreditation Authority MUST develop a specific privacy policy for the processing of personal data it undertakes as well as terms of service for its accredited users (as outlined in recommendation #11).

f) Develop a baseline application procedure: The Accreditation Authority MUST develop a uniform baseline application procedure and accompanying requirements for all applicants, requesting accreditation, including:
   i. Accreditation timeline
   ii. Definition of eligibility requirements for accredited users
   iii. Identity Validation, Procedures
   iv. Identity Credential Management Policies: lifetime/expiration, renewal frequency, security properties (password or key policies/strength), etc.

[10] For the avoidance of doubt, the code of conduct referenced here is not intended to refer to the Code of Conduct as described in the GDPR. The code of conduct referenced here refers to a set of rules and standards to be followed by the Accreditation Authority.

v. Identity Credential Revocation Procedures: circumstances for revocation, revocation mechanism(s), etc. [see also "Accredited User Revocation & abuse section below]
vi. Signed Assertions Management: lifetime/expiration, renewal frequency, etc.
vii. NOTE: requirements beyond the baseline listed above may be necessary for certain classes of Requestors.

g) Define dispute resolution and complaints process: The Accreditation Authority MUST define a dispute resolution and complaints process to challenge actions taken by the Accreditation Authority. The defined process MUST include due process checks and balances.
h) Audits: The Accreditation Authority 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 cure 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 recommendation #16).
i) User Groups: The Accreditation Authority MAY develop user groups / categories to facilitate the accreditation process as all Requestors will need to be accredited, and accreditation will include identity verification.
j) Reporting: The Accreditation Authority MUST report publicly and on a regular basis on the number of accreditation requests received, accreditation requests approved/renewed, accreditations denied, accreditations revoked, complaints received and information about the identity providers it is working with. See also recommendation #17 on reporting.
k) Renewal: The Accreditation Authority MUST establish a timeline and requirements for the renewal of the accreditation.[11]
l) Confirmation of user data: The Accreditation Authority MUST send periodic reminders (e.g., yearly) to accredited users to confirm user data and remind accredited users to keep the information required for accreditation up to date. Changes to this required information MAY result in the need to re-accredit.

1.4 Accredited User Revocation

a) 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.[12] A

[11] Implementation guidance: as a best practice, the re-accreditation period and requirements for Registrars may be considered, which is currently 5 years. For the avoidance of doubt, nothing prohibits the Accreditation Authority from requiring additional documentation upon accreditation renewal.
[12] For clarity, a legal entity would not be automatically de-accredited for the single action of an individual user whose accreditation is linked to the accreditation of the legal entity, but the entity may be held responsible for the actions of the individual user whose accreditation is linked to that of the legal entity.

non-exhaustive list of examples where revocation may apply include 1) the accredited user's violation of any applicable safeguards or terms of service, 2) a change in affiliation of the accredited user, 3) violation of data retention / destruction requirements or 4) where prerequisites for accreditation no longer exist.

b) The Accreditation Authority MUST make available an appeals mechanism to allow an accredited user to challenge the decision to revoke the accredited user's status. However, for the duration of the appeal, the accredited user's status will remain suspended. Outcomes of an appeal MUST be reported in a transparent manner**.**

c) A mechanism to report an accredited user's violation of any safeguards or terms of service MUST be provided by SSAD.[13] Reports MUST be relayed to the Accreditation Authority for handling. The Accreditation Authority MAY also obtain information from other parties in making a determination that abuse has taken place.

d) The revocation policy for individuals/entities SHOULD include graduated penalties; the penalties will be further detailed during implementation, factoring in how graduated penalties are applied in other ICANN areas. 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: i) a third-party verified complaint received; ii) results of an audit or investigation by the Accreditation Authority or auditor; iii) any misuse or abuse of privileges afforded; iv) repeated violations of the accreditation policy; v) results of audit or investigation by a DPA.

e) In the event there is a pattern or practice of abusive behavior within an entity, the credential for the entity MAY be suspended or revoked as part of a graduated sanction.

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

g) For the avoidance of doubt, De-accreditation does not prevent individuals or entities from submitting future requests under the access method provisioned in Recommendation 18 (Reasonable Requests for Lawful Disclosure) of the EPDP Phase 1 Report.

1.6 De-authorization of Identity Providers

a) The Identity providers Validation Procedures 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: i) a third-party complaint received; ii) results of an

[13] Note, abuse of SSAD by an accredited user is addressed in recommendation #13, amongst others.

audit or investigation by the Accreditation Auditor or auditor; iii) 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.

b) The Accreditation Authority MUST make available an appeals mechanism to allow an Identity Provider to challenge the decision to revoke the Identity Provider's status. However, for the duration of the appeal, the Identity Provider's status will remain suspended. Outcomes of an appeal MUST be reported in a transparent manner.

1.7 Accredited non-governmental entities or individuals:

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

b) The number of SSAD requests that can be submitted during a specific period of time MUST NOT be restricted, except where the accredited entity poses a demonstrable threat to the SSAD, or where they may be otherwise restricted under these recommendations (such as under recommendation 1.4(d) and 13(b)). It is understood that possible limitations in SSAD's response capacity and speed may apply. For further details see the response requirements recommendation.

c) MUST keep the information required for accreditation and verification up to date and inform the Accreditation Authority promptly when there are changes to this information, which MAY result in re-accreditation or re-verification of certain pieces of information provided.

Implementation Guidance

In relation to accreditation, the EPDP Team provides the following implementation guidance, with the understanding that further details will be developed in the implementation phase:

a) Recognized, applicable, and well-established organizations could support the Accreditation Authority as an Identity Provider and/or Verify information. Proper vetting, as described in 1.3(f) above, 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.[14]

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 recommendations for further details.

Recommendation #2. Accreditation of governmental entities

2.1 Objective of accreditation

SSAD MUST provide reasonable access to registration data for entities that require access to this data for the exercise of their public policy tasks. In view of their obligations under applicable data protection rules, the final responsibility for granting access to registration data will remain with the party that is considered to be a controller for the processing of that registration data that constitutes personal data.

The development and implementation of an accreditation procedure that specifically applies to governmental entities will facilitate decisions that Contracted Parties will

[14] For clarity, service providers and/or lawyers acting on behalf of trademark owners are also eligible for accreditation. However, such service providers and/or lawyers are acting on behalf (legally) of the trademark owner. Where such service providers and/or lawyers breach the rules of the SSAD, it is necessary that disclosing entities must be provided with such data, and it must be clear that such a breach may be considered in the future disclosures for trade mark owner on whose behalf the agent is acting. The use of different 3rd party agents cannot be used as a means to avoid past sanctions for misuse of the SSAD.

need to make before granting access to registration data to a particular entity or automated processing of disclosure decisions by the Central Gateway Manager, if applicable. This accreditation procedure can provide data controllers with information necessary to allow them to assess and decide about the disclosure of data.

2.2 Eligibility

Accreditation by a country's/territory's government body or its authorized body[15] would be available to various eligible government entities[16] that require access to non-public registration data for the exercise of their public policy task, including, but not limited to:

- Civil and criminal law enforcement authorities
- Data protection and regulatory authorities
- Judicial authorities
- Consumer rights organizations granted a public policy task by law or delegation from a governmental entity
- Cybersecurity authorities granted a public policy task by law or delegation from a governmental entity including national Computer Emergency Response Teams (CERTs)

2.3 Determining eligibility

Eligible government entities are those that require access to registration data for the exercise of their public policy task, in compliance with applicable data protection laws. Whether an entity should be eligible is determined by a country/territory- designated Accreditation Authority. This eligibility determination does not affect the final responsibility of the Contracted Party to determine whether or not to disclose personal data following a request for registration data or by the Central Gateway Manager in the case of requests that meet the criteria for automated processing of disclosure decisions, if applicable.

2.4 Governmental Accreditation Authority requirements

Governmental Accreditation requirements MUST follow the requirements set out in Rec. 1.3.

Additionally, the requirements MUST be listed and made available to eligible government entities. Failure to abide by these requirements may result in de-accreditation of the Accreditation Authority by ICANN Org.

[15] Implementation consideration: such a body could be an International Governmental Organization.

[16] Intergovernmental organizations (IGOs) are also eligible for accreditation under recommendation #2. An IGO that wants to be accredited MUST seek accreditation via its host country's Accreditation Authority.

2.5 Accreditation procedure

Accreditation MUST be provided by an approved accreditation authority. This authority may be either a country's/territory's governmental agency (e.g. a Ministry) or delegated to an intergovernmental organization. This authority SHOULD publish the requirements for accreditation and carry out the accreditation procedure for eligible government entities.

a. Accreditation emphasizes the responsibilities of the data Requestor (recipient), who is responsible for complying with the law.
b. Accreditation will focus on the requirements of the law, such as requirements regarding data retention length, secure storage, organizational data controls, and breach notifications.
c. Renewal, Logging, Auditing, Complaint and De-accreditation will be handled as per Rec. 1.

Implementation Guidance:

- Accreditation is required for a governmental entity to participate in the SSAD. Unaccredited governmental entities can make data requests outside the SSAD, and Contracted Parties should have procedures in place to provide reasonable access.
- Accredited users will be required to follow the safeguards as set by the policy (see also recommendation #[x] SSAD Terms and Conditions). This is without prejudice for the entity to respect safeguards under its domestic law.
- Accredited entities SHOULD provide details to aid the disclosure decision to Contracted Parties such as any applicable local law relating to the request.

Recommendation #3. Criteria and Content of Requests

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

3.2 The EPDP Team recommends that each SSAD request MUST include all information necessary for a disclosure decision, including 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, jurisdiction of Requestor);[17]

c. Information about the legal rights of the Requestor specific to the request and legitimate interest or other lawful basis and/or justification for the request, (e.g., What is the legitimate interest or other lawful basis; 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 purpose specified in (c);
e. A list of data elements requested by the Requestor, and why the data elements requested are necessary for the purpose of the request;
f. Request type (e.g. Urgent – see also recommendation #6 Priority Levels, Confidential – see also recommendation #12 – Disclosure Requirements).

3.3 The Central Gateway Manager MUST confirm that all required information is provided. Should the Central Gateway Manager detect that the request is incomplete, the Central Gateway Manager MUST notify the Requestor that the request is incomplete, detailing which required data is missing, and provide an opportunity for the Requestor to complete its request. It must not be possible for a Requestor to submit a request that is incomplete.

Implementation Guidance

The EPDP Team expects that:

- Each request needs to respond to the same questions, using the same form. While the user interface for submitting requests is considered an implementation detail, the offering of pre-populated fields, tick boxes and/or dropdown options should be considered. However, the use of pre-populated fields, tick boxes or dropdown options must not exclude the ability of Requestors from submitting free form responses.
- Requests must be in English unless the Contracted Party that is receiving the request indicates they are also willing to receive the request and/or supporting documents in other language(s).
- A signed assertion may provide one or more of the requirements as listed above.

Recommendation #4. Acknowledgement of receipt and relay of the disclosure request

4.1 Acknowledgement of receipt

[17] Consideration will need to be given by all parties involved in SSAD to the requirements that may apply to cross-border data transfers.

a. Following confirmation that the request is syntactically correct and that all required fields have been filled out, the Central Gateway Manager MUST immediately and synchronously respond with the acknowledgement of receipt and relay the disclosure request[18] to the responsible Contracted Party.
b. The response provided by the Central Gateway Manager SHOULD also include information about the subsequent steps, information on how public registration data can be obtained as well as the expected timeline consistent with the SLAs outlined in recommendation #10.

4.2 Relay of disclosure request

c. By default, the Central Gateway Manager MUST relay the disclosure request to the Registrar of Record. However, where the Central Gateway Manager is aware of any circumstance, assessed in line with these recommendations, that necessitates the provision of a disclosure request to the relevant gTLD Registry Operator, the Central Gateway Manager MAY relay the disclosure request to the relevant gTLD Registry Operator, provide that the reasons necessitating such a transfer of a request, are provided to the registry operator for their consideration. It must be possible for the Requestor to flag such circumstance to the Central Gateway Manager, but the Central Gateway Manager MUST make its own assessment of whether the identified circumstance necessitates the provision of the disclosure request to the relevant gTLD Registry Operator. For clarity, nothing in this recommendation prevents a Requestor to directly contact, outside of SSAD, the relevant gTLD Registry Operator with a disclosure request.

Implementation guidance

The EPDP Team expects that:

- The acknowledgement of receipt will include a "ticket number" or similar to facilitate interactions between the Requestor and the SSAD, details to be worked out in implementation.
- The Central Gateway Manager relays the disclosure request as well as necessary and appropriate information about the Requestor to the Contracted Party. If it concerns a disclosure requests for which automated processing of the disclosure decision applies (see recommendation Automation), the relay of the disclosure request and all relevant information may happen at the same time as the Central Gateway Manager would direct the Contracted Party to automatically disclose the requested data to the Requestor.

[18] Implementation guidance: the Central Gateway Manager is expected to relay the disclosure request as well as all relevant information about the Requestor to the Contracted Party. In the case of disclosure requests for which automated processing of the disclosure decision applies (see recommendation Automation), the relay of the disclosure request and all relevant information may happen at the same time as the Central Gateway Manager would direct the Contracted Party to automatically disclose the requested data to the Requestor.

Recommendation #5. Response Requirements

5.1 For the Central Gateway Manager:[19]

a. As part of its relay to the responsible Contracted Party, the Central Gateway Manager MAY provide a recommendation to the Contracted Party whether to disclose or not.

5.2 For Contracted Parties:

b. The Contracted Party MAY follow the recommendation of the Central Gateway Manager but is not obligated to do so. If the Contracted Party decides not to follow the recommendation of the Central Gateway Manager, the Contracted Party MUST communicate its reasons for not following the Central Gateway Manager's recommendation so the Central Gateway Manager can learn and improve on future response recommendations.

c. 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.[20] 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 in line with the SLAs described in the SLA recommendation.

d. Responses where disclosure of data (in whole or in part) has been denied MUST include a rationale sufficient for the Requestor to objectively understand the reasons for the decision, including, for example, an analysis and explanation of how the balancing test was applied[21] (if applicable). Additionally, in its response, the Contracted Party MAY include information on how public registration data can be obtained.

e. If the Contracted Party determines that disclosure would be in violation of applicable laws or result in inconsistency with these policy recommendations, the Contracted Party MUST document the rationale and communicate this information to the Requestor, and, if requested, ICANN Org.

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

[19] Note that the requirements for disclosure requests that meet the criteria for automated disclosure decisions are covered in recommendation #9.

[20] See recommendation #12 for further details on what is considered abusive use of SSAD.

[21] As per recommendation #6, care must be taken to ensure that no personal data is revealed to the Requestor within this explanation.

Org. ICANN Org MUST investigate complaints regarding disclosure requests under its enforcement processes.[22]

5.4 ICANN Compliance MUST make available an alert mechanism by which Requestors as well as data subjects whose data has been disclosed can alert ICANN Compliance if they are of the view that disclosure or non-disclosure is the result of systemic abuse by a Contracted Party. This alert mechanism is not an appeal mechanism – to contest disclosure or non-disclosure affected parties are expected to use available dispute resolution mechanisms such as courts or Data Protection Authorities – but it should help inform ICANN Compliance of potential systemic abuse which should trigger appropriate enforcement action.

Implementation Guidance

Information resulting from the alert mechanism is also expected to be included in the SSAD Implementation Status Report (see recommendation #18) to allow for further consideration of potential remedies to address abusive behavior.

It is not the EPDP Team's expectation that the Central Gateway Manager will provide a recommendation from day 1 as it is understood that experience will need to be gained before the Central Gateway Manager may be in a position to provide such a recommendation to the Contracted Party. It is the expectation that a recommendation would be developed in an automated fashion by factoring in information contained in the request, information about the Requestor, and the history of requests by the Requestor.

Recommendation #6. Priority Levels

6.1 The EPDP Team recommends that the Central Gateway Manager accommodate at least the following three (3) priority levels, which a Requestor can choose from when submitting requests through the SSAD. The priority level defines the urgency with which the disclosure request should be actioned by the Contracted Party:

[22] ICANN org would review compliance with the following: a) response adhered to established SLAs; b) response included all required content (i.e. denial communicated without disclosure of personal data, rationale for the decision, and (if applicable) how the Contracted Party applied the balancing test); c) request was reviewed based on its individual merits; and, d) absent any legal requirements to the contrary, disclosure was not refused solely for lack of any of the following: (i) a court order; (ii) a subpoena; (iii) a pending civil action; or (iv) a UDRP or URS proceeding; or solely based on the fact that the request is founded on alleged intellectual property infringement (absent any legal requirements to the contrary). Typically, ICANN Compliance will not address the merits of the request itself or the Contracted Party's conclusions, if applicable, in balancing the rights of the data subject with the legitimate interests of the requester. For avoidance of doubt, this does not preclude ICANN Org from addressing complaints related to allegations of unreasonable denials of requests to disclose data, especially where there is evidence of widespread and unjustified denials of disclosure requests.

a. **Priority 1** - Urgent Requests - The criteria to determine urgent requests is limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation. For the avoidance of doubt, Priority 1 is not limited to requests from law enforcement agencies.
b. **Priority 2** - ICANN Administrative Proceedings – disclosure requests that are the result of administrative proceedings under ICANN's contractual requirements or existing Consensus Policies, such as UDRP and URS verification requests.[23]
c. **Priority 3** - All other requests.

6.2 For Priority 3 requests, Requestors MUST have the ability to indicate that the disclosure request concerns a consumer protection issue (phishing, malware or fraud), in which case the Contracted Party MAY prioritize the request over other Priority 3 requests. Persistent abuse of this indication can result in the Requestor's de-accreditation.

6.3 The Contracted Party:

- MAY reassign the priority level during the review of the request. For example, as a request is manually reviewed, the Contracted Party MAY note that although the priority is set as priority 2 (ICANN Administrative Proceeding), the request shows no evidence documenting an ICANN Administrative Proceeding such as a filed UDRP case, and accordingly, the request should be recategorized as Priority 3.
- MUST communicate any recategorization to the Central Gateway Manager and Requestor.

6.4 The EPDP Team recommends that the SSAD MUST support 'urgent' SSAD disclosure requests to which the following requirements apply:

a. Abuse of urgent requests: Violations of the use of Urgent SSAD Requests will result in a response from the Central Gateway Manager to ensure that the requirements for Urgent SSAD Requests are known and met in the first instance, but repeated violations may result in the Central Gateway Manager suspending the ability to make urgent requests via the SSAD.
b. Contracted Parties MUST maintain a dedicated contact for dealing with Urgent SSAD Requests which can be stored and used by the Central Gateway Manager, in circumstances where an SSAD request has been flagged as Urgent. Additionally, the EPDP Team recommends that Contracted Parties MUST publish their standard business hours and accompanying time zone in the SSAD portal.

[23] For clarity, this priority assignment is expected to be limited to ICANN-approved dispute resolution service providers or its employees in the context of ICANN Administrative Proceedings.

Implementation Guidance

- See, for reference, the Framework for Registry Operator to Respond to Security Threats which notes: "*Initial judgment of a request being "High Priority" should be self-evident and require no unique skills in order to determine a public safety nexus. "High Priority" should be considered an imminent threat to human life, critical infrastructure or child exploitation".*
- Critical infrastructure means the physical and cyber systems that are vital that their incapacity or destruction would have a major detrimental impact on the physical or economic security or public health or safety.
- See also recommendation #10 which contains further details in relation to the requirements for an Urgent SSAD request.

How is priority defined?
Priority is a code assigned to requests for disclosure that contain agreed to, best effort target response times.

Who sets the priority?
The initial priority of a disclosure request is set by the Requestor, using the priority options provided by the Central Gateway Manager, based on the criteria outlined below. When selecting a priority, the Central Gateway Manager will clearly state the criteria applicable for an Urgent Request and the potential consequences of abusing this priority setting.

What happens if priority needs to be shifted?
It is possible that the initially-set priority may need to be reassigned during the review of the request. For example, as a request is manually reviewed, the Contracted Party MAY note that although the priority is set as 2 (UDRP/URS), the request shows no evidence documenting a filed UDRP case, and accordingly, the request should be recategorized as Priority 3. Any recategorization MUST be communicated to the Central Gateway Manager and Requestor. Following receipt of a non-automated disclosure request from the Central Gateway Manager, the Contracted Party is responsible for determining whether to disclose the nonpublic data. Within the above-defined response times, the Contracted Party MUST respond to the request.

Recommendation #7. Requestor Purposes

7.1 The EPDP Team recommends that:

a. Requestors MAY submit data disclosure requests for specific purposes such as but not limited to: (i) criminal law enforcement, national or public security, (ii) non law enforcement investigations and civil claims, including, intellectual property infringement and UDRP and URS claims, (iii) consumer protection,

abuse prevention, obligations applicable to digital service providers (DSP) and network security. Requestors MAY also submit data verification requests on the basis of Registered Name Holder (RNH) consent that has been obtained by the Requestor (and is at the sole responsibility of that Requestor), for example to validate the RNH's claim of ownership of a domain name registration, or contract with the Requestor.

b. Assertion of one of these specific purposes does not guarantee access in all cases, but will depend on evaluation of the merits of the specific request, compliance with all applicable policy requirements, and the legal basis for the request.

Recommendation #8. Contracted Party Authorization.

For clarity, this recommendation pertains to disclosure requests that are routed to the Contracted Party for review. These requirements DO NOT apply to disclosure requests that meet the criteria for automated processing of disclosure decisions as described in recommendation #16, regardless of whether automated processing of disclosure decisions is mandated or at the request of the Contracted Party.

General requirements

The Contracted Party

8.1. MUST review every request individually and not in bulk, regardless of whether the review is done automatically or through meaningful review and MUST NOT disclose data on the basis of accredited user category alone.

8.2. MAY outsource the authorization responsibility to a third-party provider, but the Contracted Party will remain ultimately responsible for ensuring that the applicable requirements are met.

8.3. MUST determine its own lawful basis for the processing related to the disclosure decision.[24] The Requestor will have the ability to identify the lawful basis under which it expects the Contracted Party to disclose the data requested; however, in all instances where the Contracted Party is responsible for making the decision to disclose, the Contracted Party MUST make the final determination of the appropriate lawful basis.

8.4. MUST support reexamination requests received from requests via the SSAD system and MUST consider them based on the rationale provided by the Requestor. For clarity, the resubmission of a disclosure request that is identical to the original request, without a supporting rationale as to why the request

[24] See also implementation guidance #17.

must be reconsidered, does not need to be reconsidered by the Contracted Party.

8.5. Absent any legal requirements to the contrary, disclosure MUST NOT be refused solely for lack of any of the following: (i) a court order; (ii) a subpoena; (iii) a pending civil action; or (iv) a UDRP or URS proceeding; nor can refusal to disclose be solely based on the fact that the request is founded on alleged intellectual property infringement.

Authorization determination requirements

Following receipt of a request from the Central Gateway Manager, the Contracted Party:

8.6. MUST conduct a prima facie[25] review of the request's validity, i.e., is the request sufficient for the Contracted Party to ground a substantive review and process the associated underlying data. If the Contracted Party determines that the request is not valid, e.g. it does not provide sufficient ground for a substantive review of the underlying data, the Contracted Party MAY MUST request the Requestor to provide further information prior to denying the request;

8.7. If the request is deemed valid based on the prima facie review, MUST conduct a substantive review of the request and the underlying data:

8.7.1. If, following the evaluation of the underlying data, the Contracted Party determines that disclosing the requested data elements would not result in the disclosure of personal data, the Contracted Party MUST disclose the data, unless the disclosure is expressly prohibited under applicable law.[26] For clarity, if the disclosure would not result in the disclosure of personal data, the Contracted Party does not have to further evaluate the request.

8.7.2. If following the evaluation of the underlying data, the Contracted Party determines that disclosing the requested data elements would result in the disclosure of personal data, the Contracted Party MUST determine, at a minimum, as part of its substantive review of the request and the underlying data:

8.7.2.1 whether the Contracted Party has a lawful basis for disclosure;[27]

[25] Per the Cambridge Dictionary, at first sight (based on what seems to be the truth when first seen or heard).
[26] When considering the publication of non-public data of legal persons, particularly with respect to NGOs and parties engaged in human rights activities that may be protected by local law (e.g. Constitutional and Charter Rights law), the Contracted Party should consider the impact on individuals that could potentially be identified by disclosing the legal person data.
[27] See also implementation guidance #17

8.7.2.2 whether all the requested data elements are necessary;[28]
8.7.2.3 whether balancing or review is required under applicable law.

8.8. If the request is subject to balancing or review as per paragraph 7.2.:
- 8.8.1 MUST disclose the data if, based on its evaluation, the Contracted Party determines that the Requestor's legitimate interest is not outweighed by the interests or fundamental rights and freedoms of the data subject. The Contracted Party MUST document the rationale for its approval.
- 8.8.2 MUST deny the request, if, based on its evaluation, the Contracted Party determines that the Requestor's legitimate interest is outweighed by the interests or fundamental rights and freedoms of the data subject. The Contracted Party MUST document the rationale for its denial and MUST communicate the reason for denial to the Central Gateway Manager, with care taken to ensure no personal data is included in the reason for denial.

8.9. If the request is not subject to balancing or review as per paragraph 7.2.:
- 8.9.1 MUST disclose if the Contracted Party determines it has a lawful basis or is not prohibited under applicable law to disclose the data. The Contracted Party MUST document the rationale for its approval.
- 8.9.2 MUST deny the request if the Contracted Party determines it does not have a lawful basis or is prohibited under applicable law to disclose the data. The Contracted Party MUST document the rationale for its denial and MUST communicate the reason for denial to the Central Gateway Manager, with care taken to ensure no personal data is included in the reason for denial.

The Requestor:

8.10. MAY file a reexamination request if it believes its request was improperly denied.

8.11. MUST, within its reexamination request, provide a supporting rationale as to why its request must be reexamined. The supporting rationale should provide sufficient detail as to why the Requestor believes its request was improperly denied.

8.12. If a Requestor believes a Contracted Party is not complying with any of the requirements of this policy, the Requestor SHOULD notify ICANN Compliance further to the alert mechanism described in Recommendation #5 – Response Requirements.

[28] For further context regarding the definition of necessary, please refer to p. 7 of the legal guidance the EPDP Team referenced when formulating this definition.

Implementation Guidance

8.13. The EPDP Team envisions the Contracted Party having the ability to communicate with the Requestor via a dedicated ticket in the SSAD. The EPDP Team also envisions the SSAD offering encryption to protect the transmission of personal data.

8.14. The EPDP Team notes the specifics of how the communication in paragraph 6 will be assessed in the policy implementation phase; however, the EPDP Team provides this additional guidance to assist. The EPDP Team envisions the Contracted Party sending a notice to the Requestor, via the relevant SSAD ticket, noting its decision to deny the request. The Requestor would then have (x) amount of days to provide updated information to the Contracted Party. Upon the Requestor's provision of updated information, the SLA response time would reset. For example, the Contracted Party would have 1 business day to respond to the updated urgent request. If the Requestor chooses not to provide the information, the SLA would be counted when the Contracted Party sends the "intent to deny" notice to the Requestor. If the Requestor decides not to respond, the request is denied as soon as the time period has expired.

8.15. In situations where the Contracted Party is evaluating the legitimate interest of the Requestor, the Contracted Party SHOULD consider the following:

8.15.1 Interest must be specific, real, and present rather than vague and speculative.

8.15.2 An interest is generally deemed legitimate so long as it can be pursued consistent with data protection and other laws.

8.15.3 Examples of legitimate interests include: (i) enforcement, exercise, or defense of legal claims, including IP infringement; (ii) prevention of fraud and misuse of services; (iii) physical, IT, and network security.

8.16. The Contracted Party SHOULD[29], as part of its substantive review, assess at least:

[29] ICANN org would review compliance with the following: a) response adhered to established SLAs; b) response included all required content (i.e. denial communicated without disclosure of personal data, rationale for the decision, and (if applicable) whether the Contracted Party applied the balancing test); c) request was reviewed based on its individual merits; and, d) absent any legal requirements to the contrary, disclosure was not refused solely for lack of any of the following: (i) a court order; (ii) a subpoena; (iii) a pending civil action; (iv) a UDRP or URS proceeding; or (e) denials where the registration data does not include personal information. Note, (e) shall neither predetermine nor contradict any outcome of the legal / natural discussion, the result of which shall prevail this clause. Typically, ICANN Org will not be in a position to address the merits of the request itself or the Contracted Party's conclusions, if applicable, in balancing the rights of the data subject with the legitimate interests of the requester. For avoidance of doubt, this does not preclude ICANN Org from addressing complaints related to allegations of unreasonable denials of requests to disclose data, especially where there is evidence of widespread and unjustified denials of disclosure requests. the legal discretion of the Contracted Party making the determination based on these policy recommendations.

8.16.1 Where applicable, the following factors should be used 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 Contracted Party SHOULD consider the totality of the circumstances outlined below:

8.16.1.1 *Assessment of impact*. Consider the direct impact on data subjects as well as any broader possible consequences of the data processing. Consider the public interest and legitimate interests pursued by the Requestor to, for example, maintain the security and stability of the DNS. Whenever the circumstances of the disclosure request or the nature of the data to be disclosed suggest an increased risk for the data subject affected, this shall be taken into account during the decision-making.

8.16.1.2 *Nature of the data.* Consider the level of sensitivity of the data as well as whether the data is already publicly available.

8.16.1.3 *Status of the data subject.* Consider whether the data subject's status increases their vulnerability (e.g., children, asylum seekers, other protected classes)

8.16.1.4 *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),[30] provided that this is not intended to prohibit public disclosures for legal actions or administrative dispute resolution proceedings such as the UDRP or URS.

8.16.1.5 *Reasonable expectations of the data subject.* Consider whether the data subject would reasonably expect their data to be processed/disclosed in this manner.

8.16.1.6 *Status of the controller and data subject.* Consider negotiating power and any imbalances in authority between the controller and the data subject.[31]

8.16.1.7 *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.

8.16.1.8 *Cross-border data transfers.* Consider the requirements that may apply to cross-border data transfers.

[30] For further context regarding the higher risk when data is combined, please refer to p. 5 of the legal guidance the EPDP Team referenced when considering these factors.

[31] In the context of Contracted Party authorization, the relevant parties are the Contracted Party (controller) and the registrant (data subject); however, the roles and responsibilities of the parties will be further discussed in implementation.

8.17. A lawful basis may be based on either the presence of a lawful basis under applicable law; or on the absence of a prohibition on the processing and disclosure of the data requested under applicable law.

The application of the balancing test and factors considered in this section SHOULD be revised, as appropriate, to address applicable case law interpreting GDPR, guidelines issued by the EDPB or revisions to GDPR or other applicable privacy laws that may occur in the future.

Recommendation #9. Automation of SSAD Processing

9.1. The EPDP Team recommends that the Central Gateway manager MUST automate the receipt, authentication, and transmission of SSAD requests to the relevant Contracted Party insofar as it is technically and commercially feasible and legally permissible.

9.2. The SSAD MUST allow for the automation of the processing of well-formed, valid, complete, properly identified requests from accredited users as described below.

Automated processing of disclosure decisions

9.3. Contracted Parties MUST process in an automated manner disclosure decisions for any categories of requests for which automation is determined (see 16.4 and the processes detailed in recommendation #19) to be technically and commercially[32] feasible[33] and legally permissible. For the avoidance of doubt, the EPDP Team recommends that any categories of disclosure decisions that do not currently meet these criteria will not be foreclosed from consideration of automated disclosure in the future, subject to the processes detailed in Recommendation #19. In areas where disclosure decisions do not meet these criteria, standardization of the disclosure decision process is the baseline objective.

9.4. Per the legal guidance obtained (see here), the EPDP Team recommends that the following types of disclosure requests are legally permissible under GDPR for full automation (in-take as well as processing of disclosure decision) from the start:

[32] During implementation, further consideration will need to be given to the commercial feasibility for registrars that may receive a very limited number of requests that will meet the criteria for automated processing of disclosure decisions and whether the financial burden of enabling this automated processing is of such a nature that an exemption may need to be provided. As part of this consideration, the Central Gateway Manager also should consider how it can facilitate the integration of a Contracted Party's system with the SSAD to reduce any potential burden of automated processing of disclosure decisions.

[33] Initial consideration of the financial feasibility of automation will be addressed by ICANN org with the Implementation Review Team and subsequently by the mechanism for the evolution of SSAD, as applicable.

- Requests from Law Enforcement in local or otherwise applicable jurisdictions with either 1) a confirmed GDPR 6(1)e lawful basis or 2) processing is to be carried out under an Article 2 exemption;
- Investigation of data protection infringement allegedly affecting a registrant by a data protection authority;
- Request for city field only, to evaluate whether to pursue a claim or for statistical purposes;
- No personal data on registration record that has been previously disclosed by the Contracted Party.

9.5. For clarity, if a Contracted Party determines that automated processing of disclosure decisions for the use cases specified in this recommendation or through the processes detailed in Recommendation #18 is not legally permissible or brings with it a significant risk that was not recognized in the legal guidance obtained by the EPDP Team but has been subsequently identified and documented through, for example, a Data Protection Impact Assessment (DPIA), the Contracted Party MUST notify including supporting documentation ICANN org it requires an exemption from automated processing of disclosure decisions for the identified use case(s). Unreasonable exemption notifications MAY be subject to review by ICANN Org. ICANN org MUST reverse the exemption recognition if it finds the Contracted Party notification incorrect or abusive.

9.6. As soon as ICANN org has been notified, the Central Gateway Manager MUST halt the transmission of the identified use cases as requiring automated processing and MUST transmit the request pursuant to the requirements in Recommendation 8 – Contracted Party Authorization.

9.7. ICANN org MUST provide a notice and comment process to allow affected stakeholders to provide input on the exemptions provided for in paragraph 5. ICANN org MAY facilitate a subsequent discussion between affected stakeholders and the Contracted Party in question to facilitate mutual understanding of the exemption and supporting information. Further details will be determined in implementation, including potential confidentiality of the process.

9.8. As soon as the Contracted Party becomes aware that the exemption is no longer applicable, it MUST inform ICANN org accordingly.

9.9. Following a Contracted Party's notification under paragraph 8, the Central Gateway Manager MUST transmit requests that meet the criteria for automated processing to the Contracted Party in accordance with this recommendation and the Contracted Party MUST resume automated processing of disclosure decisions for the relevant use cases.

9.10. With respect to disclosure requests that would be sent to a Contracted Party for review, a Contracted Party MAY request the Central Gateway to automate the processing of the disclosure decision of all, or certain types of, disclosure requests and/or requests coming from a certain Requestor,[34] after the Contracted Party has weighed the risk and assessed the legal permissibility, as applicable.

9.11. A Contracted Party MAY retract or revise a request for automating the disclosure decision that is not required by these policy recommendations at any time.

9.12. For clarity, the Central Gateway Manager oversees whether a disclosure decision has met the criteria for automated processing of disclosure decisions which MAY involve non-automated review at the Central Gateway. Similarly, the Central Gateway MAY request the Contracted Party for further information that may help the Central Gateway Manager in determining whether or not the criteria for an automated processing of disclosure decisions have been met. A Contracted Party MAY provide such further information, if requested. There is no expectation that personal data is transferred in response to such an information request.

Implementation Guidance

In addition to the requirements detailed in Recommendation #4 (Acknowledgement of Receipt) and Recommendation #8 (SLAs), which will also apply to automated processing of disclosure decisions, the following implementation guidance will apply to automated processing of disclosure decisions, i.e., requests for which the Central Gateway Manager determines an automated decision to the disclosure request from the Contracted Party is required, as per this recommendation.

9.13. 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 is likely not possible to completely automate all aspects of disclosure request review and disclosure in all cases.

9.14. In the context of further consideration of potential use cases that are deemed legally permissible in the context of recommendation #18, legally permissible is expected to be determined, in the absence of authoritative guidance (e.g. EDPB, European Court of Justice (ECJ), new law), by the

[34] For example, a Contracted Party could consider implementing a Trusted Notifier scheme that would allow qualification of Requestors that meet certain criteria established by the relevant Contracted Party to obtain automated responses to their disclosure requests.

party/parties bearing liability for the automated processing of disclosure decisions.

9.15. Further to the legal guidance referenced above, the EPDP Team recommends the GNSO Standing Committee (see recommendation #18), in its review, further consider both the safeguards outlined in appendix 2 of the legal memo and the use cases outlined in Section 3.4 of the legal memo, to consider whether disclosure would constitute a legal or similar significant effect, which might prevent automation of disclosure.

9.16. The way automated processing of disclosure decisions is expected to work in practice is that the Central Gateway Manager would confirm the request meets the requirements for automated processing and direct the Contracted Party to automatically disclose the requested data to the Requestor. This could be done in the form of a command via a secure mechanism or some other way that is to be determined during implementation.

9.17. Consideration will need to be given by all parties involved in SSAD to the requirements that may apply to cross-border data transfers.

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

10.1. The EPDP Team recommends that Contracted Parties MUST abide by Service Level Agreements (SLAs) that are developed, implemented, and enforced, and as updated from time to time per Recommendation #18, in accordance with the implementation guidance provided below.

10.2. For purposes of calculating SLA response time, the EPDP Team recommends the SLA starts when a validated request with all supporting information is provided to the Contracted Party by the Central Gateway Manager and stops when the Contracted Party responds (via the Central Gateway) with either the information requested, a rejection response, or a request for additional information. A reexamination request or a Requestor response with more information would be considered the start of a new request for SLA calculation purposes.

Priority Matrix for non-automated disclosure requests

Request Type	Priority	Proposed SLA[35] (Compliance at 6 months / 12 months / 18 months)

[35] Note, the business days referenced in the table are from the moment of Contracted Party receipt of the disclosure request from the Central Gateway Manager.

Urgent Requests	1	1 business day, not to exceed 3 calendar days (85% / 90% / 95%)
ICANN Administrative proceedings	2	Max. 2 business days (85% / 90% / 95%)
All other requests*	3	See implementation guidance below.

*Note: Nothing in these policy recommendations explicitly prohibits the development of new categories and defined SLAs.

Implementation Guidance

Proposed Definitions

Business days: as defined in the jurisdiction of the Contracted Party.
Mean Response Time: A rolling average of all response times, automatically calculated frequently (e.g. daily or weekly) as a utility to a Contracted Party to evaluate their own performance at any time.
Response Target Evaluation Interval: A 3-month period allowing for review of response time performance 4 times per year.
Response Target Value: The value of the Mean Response Time measurement on the closing day of the Response Target Evaluation Interval.

Contracted Party response time requirements for SSAD requests will occur over two phases:

- Phase 1 begins **six (6) months** following the SSAD Policy Effective Date.
- Phase 2 begins **one (1) year** following the SSAD Policy Effective Date.

PHASE 1 (only applies to priority 3 requests)

10.3. During Phase 1, Contracted Party response targets for SSAD Priority 3 requests will be five (5) business days.

10.4. The Central Gateway Manager MUST measure response targets using a Mean Response Time, not on a per-response basis.

10.5. The SSAD MUST calculate Contracted Party's ongoing Mean Response Time as a rolling average, as a utility to a Contracted Party to evaluate their own performance at any time.

10.6. The SSAD MUST also measure the Response Target Value of the ongoing rolling average at the end of the Response Target Evaluation Interval. Only the 3-month Response Target Value MUST be used to determine success or failure to

meet response targets as described below. For the avoidance of doubt, the intent of the SSAD providing the Contracted Party with the Mean Response Time is to provide a warning to the Contracted Party that there may be an issue with its response times and to allow the Contracted Party to remedy the issue in a cooperative manner. During Phase 1, if the Contracted Party's Response Target Value exceeds five (5) business days, this MUST NOT result in a policy breach.

Instead, failure to meet a response target will prompt ICANN to alert the Contracted Party of a response target failure.

10.7. The Contracted Party MUST respond to the ICANN's response target failure notice within five (5) business days.

10.8. The Contracted Party's response must include a rationale as to why the Contracted Party could not meet its response target.

10.9. Failure of the Contracted Party to respond to ICANN's notice MUST be considered a breach of the policy; accordingly, the failure to respond to the compliance notice will result in an ICANN Compliance inquiry.

PHASE 2 (only applies to priority 3 requests)

10.10. In Phase 2, Contracted Party compliance targets for SSAD Priority 3 requests will be ten (10) business days.

10.11. The Central Gateway Manager MUST measure compliance targets using a mean response time, not on a per-response basis. The SSAD will calculate Contracted Party's mean compliance target on the final day of the Response Target Evaluation Interval.

10.12. If the Contracted Party's Response Target Value exceeds ten business days, this will result in a policy breach, and, accordingly, the Contracted Party will be subject to compliance enforcement.

10.13. Response Targets and Compliance Targets MUST be reviewed, at a minimum, after every six months in the first year, thereafter annually (depending on the outcome of the first review).

10.14. Response targets for disclosure requests that meet the criteria for fully-automated responses are expected to be further developed during the implementation phase, but these are expected to be under 60 seconds.

10.15. The Implementation Review Team should further consider the effect of the SLAs in instances where additional information is requested from the Contracted Party and provided by the Requestor. (Please see Recommendation #8 Contracted Party Authorization for additional information.)

Recommendation #11. SSAD Terms and Conditions

11.1. The EPDP Team recommends that minimum expectations for appropriate agreements and policies, such as terms of use for the SSAD, an SSAD privacy policy, disclosure agreement and an acceptable use policy are further defined during the implementation phase, to be subsequently developed and enforced by the entity responsible for the SSAD (by ICANN Org or a third party that has been tasked by ICANN Org to take on this enforcement function). These agreements and policies MUST take into account the recommendations from the other recommendations. These agreements and policies are expected to be developed and negotiated, as appropriate, by the parties involved in SSAD, taking the below implementation guidance into account.

11.2. The SSAD Terms and Conditions MAY be updated as appropriate by ICANN org to address applicable law and practices.

Implementation guidance:

a. Privacy Policy for processing of personal data of SSAD Users (SSAD Requestors and Contracted Parties) by SSAD

The EPDP recommends, at a minimum, the privacy policy SHALL include relevant data protection principles, including:

- 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
- Transparency requirements
- Data security requirements
- Accountability measures (privacy by design, by default, DPO above certain size, etc)

b. Terms of Use for SSAD users (SSAD Requestors and Contracted Parties)

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

- Requestor's indemnification of the controllers (entity responsible for disclosure decision) based on the following principles:
  - Requestors are responsible for damages or costs related to third party claims arising from (i) their misrepresentations in the accreditation or request process; or (ii) misuse of the requested data in violation of the applicable terms of use or applicable law(s).
  - Nothing in these terms limits any parties' liability or rights of recovery under applicable laws (i.e. Requestors are not precluded from seeking recovery from controllers where those rights are provided under law).
  - Nothing in these terms shall be construed to create indemnification obligations for public authority Requestors who lack the legal authority to enter into such indemnification clauses. Further, nothing in this clause shall alter potentially existing government liability as a recourse for the operators of the SSAD.
- Data request requirements
- Logging and audit requirements
- Ability to demonstrate compliance
- Applicable prohibitions
- Abuse prevention requirements

c. Disclosure agreements for SSAD Requestors

The EPDP recommends, at a minimum, disclosure agreements SHALL address the requirements for Requestors after data has been disclosed to the Requestor:

- 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 and destruction of data: 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, unless otherwise required to retain such data for a longer period under applicable law.
- Lawful use of data

d. Acceptable Use Policy for SSAD Requestors. The Requestor MUST accept the Acceptable Use Policy before disclosure requests can be submitted through SSAD.

At a minimum, the Acceptable Use Policy MUST include the following requirements:

The Requestor:

b) MUST only request data from the current RDS data set (no historic data);
c) MUST, for each 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 recommendation #16 for further details);
d) MAY request data from the SSAD for multiple purposes per request, for the same set of data requested;
e) 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 recommendation #16 further details).

Recommendation #12. Disclosure Requirement

12.1. The EPDP Team recommends:

Contracted Parties:
a. MUST only disclose the data requested by the Requestor;
b. MUST return current[36] data or a subset thereof (no historic data);

Contracted Parties and the Central Gateway Manager:
c. MUST process data in compliance with applicable law;
d. Where required by applicable law, MUST disclose to the Registered Name Holder (data subject), on reasonable request, confirmation of the processing of personal data relating to them, noting, however, the nature of legal investigations or procedures[37] MAY require SSAD and/or the disclosing entity to keep the nature or existence of certain requests confidential from the data subject. Confidential requests MAY be disclosed to data subjects in cooperation with the requesting entity, and in accordance with the data subject's rights under applicable law;
e. Where required by applicable law, MUST provide mechanism under which the data subject may exercise its right to erasure, to object to automated processing of its personal information should this processing have a legal or similarly significant effect, and any other applicable rights;

[36] Implementation guidance: Current data means the data reviewed by the Contracted Party when making the determination whether to disclose the data. In order to lower the possibility of changes to the data during the pendency of an outstanding disclosure request, e.g., if the registrant updates its contact data, Contracted Parties are encouraged to disclose data as soon as possible following its decision on whether to disclose. For the avoidance of doubt, historic data refers to the registration data in place before the request for disclosure was made, not registration data that may have changed as a result of any updates made by the registrant between the time the request for disclosure is reviewed and the decision to disclose the registration data.

[37] Implementation guidance: the nature of legal investigations or procedures are not limited to criminal investigations or to other investigations (e.g. many civil investigations require confidentiality).

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

Recommendation #13. Query Policy

13.1 The EPDP Team recommends that the Central Gateway Manager:

a. MUST monitor the system and take appropriate action,[38] 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[39] 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 Central Gateway Manager makes a determination based on abuse to limit the number of requests from a Requestor, further to point b, the Requestor MAY seek

[38] The EPDP Team expects that 'appropriate action' will be further defined in the implementation phase. Implementation guidance: Abusive behavior can ultimately result in suspension or termination of access to the SSAD; however, a graduated penalty scheme should be considered in implementation. There may, however, be certain instances of egregious abuse, such as counterfeiting or stealing credentials, where termination would be immediate.

[39] The EPDP Team expects that 'high volume' will be further defined in the implementation phase.

redress[40] via ICANN org if it believes the determination is unjustified. For the avoidance of doubt, if the SSAD receives a high volume of requests from the same Requestor, the volume alone must not result in a de facto determination of system abuse.

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[41] each request on its own merits.[42]

13.2. The EPDP Team recommends that Contracted Parties:

d. MUST NOT reject disclosure requests from SSAD on the basis of abusive behavior which has not been determined abusive by the Central Gateway Manager as per a) and b) above.

13.3. The EPDP Team recommends:

- The Central Gateway Manager MUST support requests keyed on fully qualified domain names (without wildcards).
- The Central Gateway Manager MUST support the ability of a Requestor to submit multiple domain names in a single request.[43]
- For disclosure requests that are not subject to the automated processing of the disclosure decision, the Central Gateway Manager MUST route each domain individually to the Contracted Party responsible for the disclosure decision (this may require SSAD to split a request into multiple transactions).
- Notwithstanding the recommendations relating to the management of abusive behavior, the Central Gateway Manager and Contracted Parties MUST have the capacity to handle a reasonable number of requests in alignment with the SLAs established.
- The Central Gateway Manager MUST only support requests for current data (no data about the domain name registration's history).
- The SSAD MUST be able to save the history of the different disclosure requests, in order to keep traceability of exchanges between the SSAD Requestors and Contracted Parties via the SSAD. Appropriate safeguards need to put in place to safeguard this information. Appropriate access to such relevant activity statistics should be provided to the CPs, as deemed necessary,[44] to ensure that

[40] For clarity, redress would be in the form of reconsideration by the Central Gateway Manager, for which the Requestor may provide new information but is not required to do so.
[41] It is the expectation that this examination is done automatically.
[42] For clarity, 'on its own merits' means that requests cannot be considered in bulk but must be considered individually, regardless of whether the consideration is done automatically or through meaningful review.
[43] The EPDP Team expects implementation to reasonably determine how many may be submitted at a time, consistent with the Query Policy. Implementation guidance: an SSAD request must be received for each domain name registration for which non-public registration is requested to be disclosed but 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 provided that the same request information applies.
[44] Implementation guidance: this is expected to be limited to a CP's own activity.

all relevant information relating to requests for disclosure are available for consideration in such disclosure decisions.

See also the Acceptable Use Policy requirements in recommendation #11 – Terms and Conditions.

Recommendation #14. Financial Sustainability

14.1. 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.

14.2. The objective is that the SSAD is financially self-sufficient without causing any additional fees for registrants. Data subjects MUST NOT bear the costs for having data disclosed to third parties;[45] Requestors of the SSAD data should primarily bear the costs of maintaining this system. Furthermore, Data Subjects MUST NOT bear the costs of processing of data disclosure requests, which have been denied by Contracted Parties following evaluation of the requests submitted by SSAD users. ICANN MAY contribute to the (partial) covering of costs for maintaining the Central Gateway.[46]

14.3. The SSAD SHOULD NOT be considered a profit-generating platform for ICANN or the contracted parties. Funding for the SSAD should be sufficient to cover costs, including for subcontractors at fair market value and to establish a legal risk fund.[47] 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.

14.4. In relation to the accreditation framework:

a. Accreditation applicants MUST be charged a to-be-determined non-refundable fee proportional to the cost of validating an application, except under certain circumstances these fees may be waived or zero for certain

[45] For clarity, the EPDP Team understands that registrants are ultimately the source of much of ICANN's revenue, as such "Data subjects MUST NOT bear the costs for having data disclosed to third parties" is not considered in violation. This language means that data subjects must not be charged a separate fee by the Central Gateway for having their data requested by or disclosed to third parties. However, the EPDP Team notes that registered name holders will always indirectly bear any costs incurred by registrars and registries. The EPDP Team also understands that the RAA prohibits ICANN from limiting what Registrars may charge. RAA 3.7.12 states: "Nothing in this Agreement prescribes or limits the amount Registrar may charge Registered Name Holders for registration of Registered Names."

[46] Although it is understood that registrants are ultimately the source of much of ICANN's revenue, this is not deemed to be a violation of "Data subjects MUST NOT bear the costs for having their data disclosed to third parties".

[47] Given the potential for legal uncertainty and the heightened legal and operational risk on all parties included in the provision of the SSAD, creation of a legal risk fund refers to the creation of a suitable legal contingency plan, including but not limited to appropriate insurance cover, and any other appropriate measures that may be deemed sufficient to cover potential regulatory fines or related legal costs.

types or categories of applicants which SHOULD be further defined during the implementation phase.

b. Rejected applicants MAY re-apply, but the new application(s) MAY be subject to the application fee.

c. Fees are to be established by the accreditation authority. If the Accreditation Authority outsources the Identity Provider function, the Identity Provider MAY establish its own fees after consulting the Accreditation Authority.

d. Accredited users and organizations MUST renew their accreditation periodically.

Implementation Guidance

14.5. 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,[48] Contracted Parties and other parties that may be involved.[49] As part of the operationalization of SSAD, ICANN org is expected to consider building on existing mechanisms or using an RFP process to reduce costs rather than building the SSAD and its components from scratch. 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 as a measure of commercial and technical feasibility.

14.6. The subsequent running of the system is expected to happen on a cost recovery basis whereby historic costs[50] 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 costs of running the SSAD may be offset by charging fees to the users of the SSAD.

14.7. When implementing and operating the SSAD, a disproportionately high burden on smaller operators should be avoided.

14.8. The EPDP Team recognizes that the fees associated with using the SSAD may differ for users based on request volume or user type among other potential factors. The EPDP Team also recognizes that governments may be subject to certain payment restrictions, which should be taken into account as part of the implementation.

[48] See also the input that ICANN Org provided at the EPDP Team's request in relation to the cost estimate for a Proposed System for Standardized Access/Disclosure (see https://community.icann.org/x/GIIEC)

[49] For clarity, ICANN org will bear its own costs for developing the system. Contracted Parties will be responsible for their own costs.

[50] Historic costs refer to the costs for developing, deployment, and operationalizing of the system.

Implementation guidance: (associated with disclosure requests):

14.9. There are various implementation details that may have policy implications, particularly with respect to cost distribution and choice of party who performs various data protection functions. These issues are collected here under Implementation Guidance for consideration.

14.10. 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 SSAD fee structure may need to be reviewed over time.

Recommendation #15. Logging

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

- Accreditation authority
- Central Gateway Manager
- Identity provider
- Contracted Parties
- Activity of accredited users such as login attempts, queries
- What queries and disclosure decision(s) are made

15.2. The EPDP Team recommends:

a. The Central Gateway Manager shall make logs of all activities of all entities which interact with the Central Gateway Manager (for further details, please see below).
b. Logs MUST 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 SHOULD NOT contain any personal information. If any information is logged that does contain personal information, appropriate safeguards need to be in place. Logs may be made publicly available as long as any personal information has been removed (see also recommendation #NEW on reporting requirements). Logged data that contains personal information MUST remain confidential.
e. Logs MUST be retained in a commonly used,[51] machine-readable format accompanied by an intelligible description of all variables.

[51] For clarity, "commonly" is intended to mean a format that is used by many, as opposed to a uniform format for all.

f. Relevant logged data MUST be disclosed, when legally permissible, in the following circumstances:
- In the event of a claim of misuse, logs may be requested for examination by an accreditation authority or dispute resolution provider.
- Logs should be further available to ICANN and the auditing body.
- When mandated as a result of due legal process, including relevant enforcement and regulatory authorities, as applicable.

Relevant logged data MAY be disclosed for:
- General technical operation to ensure proper running of the system.

Relevant logs should be used as the source to make available any relevant data. This data should enable Requestors and Contracted Parties to review their own statistics.

15.3. At a minimum, the following events MUST be logged:
- Logging related to the Identity Provider[52]
- Logging related to the Accreditation Authority
  - 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 Signed Assertions have been Validated.
  - Unique reference number
- Logging related to the Central Gateway Manager
  - 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)
  - Rates of:
    - disclosure and non-disclosure;
    - use of each reason for denial for non-disclosure;
    - divergence between the disclosure and non-disclosure decisions of a CP and the recommendations of the Central Gateway.
- Logging related to Contracted Parties
  - Request Response details, e.g., Reason for denial, notice of approval and data fields released. Disclosure decisions including a reason for denial must be stored.

Recommendation #16. Audits

[52] To be further detailed in the implementation phase.

16.1. The EPDP Team recommends that the appropriate auditing processes and procedures MUST be put in place to ensure appropriate monitoring and compliance with the requirements outlined in these recommendations.

16.2. 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 Accreditation Authority

16.3. 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 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. ICANN org as the Accreditation Authority is not required to audit governmental entities, whose accreditation and audit requirements are defined in Recommendation #2.

16.4. 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.

16.5. As part of such audits, the accreditation authority MUST 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.

16.6. If ICANN serves as the accreditation authority, existing accountability mechanisms are expected to address any breaches of the accreditation policy, noting that in such an extreme case, the credentials issued during the time of the breach will be reviewed. Modalities of this review SHOULD be established in the implementation phase.

Audits of Identity Provider(s)

16.7. Identity Providers MUST be audited periodically to ensure compliance with the policy requirements as defined in the accreditation 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.

16.8. Any audit of an Identity Provider MUST 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.

16.9. As part of such audits, the Identity Provider MUST 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

16.10. 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 recommendation #16. These could include, for example, audits triggered by verified 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 and/or Identity Provider, if applicable, for action.

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

16.12. As part of such audits, the accredited entity/individual MUST, 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.

Recommendation #17. Reporting Requirements

17.1. The EPDP Team recommends that ICANN org establish regular public reporting on the use and functioning of the SSAD. For the avoidance of doubt, this recommendation does not intend to prevent ICANN org from conducting additional non-public reporting to SSAD users.

Implementation guidance:

The EPDP Team recommends that further consideration is given during implementation to:

- The frequency of public reporting – public reporting on a quarterly basis would be considered reasonable;
- Data to be reported on, which is expected to include information such as: a) number of disclosure requests; b) disclosure requests per category of Requestors; c) disclosure requests per Requestor (for legal entities); disclosure requests granted / denied, and; response times. Please note that this is a non-exhaustive list.
- Mechanism for public reporting – consider the possibility of a publicly-available dashboard instead of or in addition to reports that are posted;
- Needs for possible confidentiality in certain cases such as information about natural persons and LEA requests. Aggregate data or pseudonymization could be considered to address possible confidentiality concerns.

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

18.1. The EPDP Team recommends that a GNSO Standing Committee be established to evaluate SSAD operational issues emerging as a result of adopted ICANN Consensus Policies and/or their implementation. The GNSO Standing Committee is intended to examine data being produced as a result of SSAD operations, and provide the GNSO Council with Recommendations on how best to make operational changes to the SSAD, which are strictly implementation measures, in addition to Recommendations based on reviewing the impact of existing Consensus Policies on SSAD operations.

18.2. No earlier than 3 months and no later than 9 months after the operationalization of SSAD, ICANN org will publish an SSAD Status Report or dashboard, and continue to do so on a quarterly basis, that will include at a minimum:

- Number of disclosure requests received;
- Average response times to the disclosure requests, categorized by priority level;
- Number of requests categorized by third-party purposes / justifications (as identified in recommendation #4);
- Number of disclosure requests approved and denied;
- Number of disclosure requests automated;
- Number of requests processed manually;
- Information about financial sustainability of SSAD;
- New EDPB guidance or new topical jurisprudence (if any);
- Technical or system difficulties;

- Operational and system enhancements.

18.3. The EPDP Team also recommends that the following principles be used as the basis by which the GNSO Standing Committee shall conduct its mission, which must be reflected in its charter:

a. Composition: The composition of the GNSO Standing Committee shall be representative of the ICANN Advisory Committees and GNSO Stakeholder Groups and Constituencies represented in the current EPDP Team on the Temporary Specification for gTLD Registration Data. This composition shall include at least one member from the GAC, ALAC, SSAC, RySG, RrSG, NCSG, IPC, BC and ISPCP, as well as at least one alternate member from each group. Note, the number of members per group should not impact the consensus designation process as positions are expected to be considered per group and not at the individual member level. The GNSO Council may also consider inviting ICANN org liaisons as members to the GNSO Standing Committee.

b. Scope: A Charter must be developed by the GNSO Council in conjunction with Advisory Committees, e.g., GAC, SSAD, and ALAC for the GNSO Standing Committee. The Charter must allow the Committee to address any operational issues involving the SSAD. This may include, but is not limited to, topics such as Service Level Agreements (SLAs), automation, third party purposes, financial sustainability and operational / system enhancements. The threshold for accepting an issue being on the GNSO Standing Committee's agenda shall be low enough to allow any of the groups involved the ability to have their interests in SSAD operations seriously considered by the Committee. Identification of issues, which the Committee may address shall be determined using the following two methods:
i. Any policy or implementation topic concerning SSAD operations may be raised by a member of the GNSO Standing Committee, and shall be placed on the Committee's working agenda if seconded by at least one other Committee member.
ii. Additionally, the GNSO Council may identify SSAD operational issues. The GNSO Council may choose to task the GNSO Standing Committee with evaluation of issues it identifies, in order for the Committee to provide the Council with consensus recommendations by the affected stakeholders on how best to address them.

Recommendations concerning implementation guidance shall be sent to the GNSO Council for consideration and adoption, after which they will be sent to ICANN for further implementation work. Recommendations which require changes being made to existing ICANN Consensus Policies shall be recorded and

maintained, to be used in the issues scoping phase of future policy development and/or review.

c. Required Consensus: Consensus Level for GNSO Standing Committee Recommendations: Recommendations on SSAD operations and policies developed by the Standing Committee must achieve consensus of the members of the Committee in order to be sent as formal recommendations to the GNSO Council. For recommendations to achieve a consensus designation, the support of the Contracted Parties will be required. For the purpose of assessing level of consensus, Members are required to represent the formal position of their SG/C or SO/AC, not individual views or positions.

d. Disbanding the GNSO Standing Committee: The Standing Committee may recommend to the GNSO Council that the Committee itself be disbanded, should the need arise. In order for the Standing Committee to recommend to the GNSO Council that it be disbanded, an affirmative vote of a simple majority of the groups involved is required. This recommendation would subsequently need to be adopted by the GNSO Council.

3.6 EPDP Team Priority 2 Recommendations

Recommendation #19. Display of information of affiliated privacy / proxy providers

In the case of a domain name registration where an accredited privacy/proxy service is used, e.g., where data associated with a natural person is masked, Registrar (and Registry, where applicable) MUST include the full RDDS data of the accredited privacy/proxy service in response to an RDDS query. The full privacy/proxy RDDS data may also include a pseudonymized email.

Implementation notes:

1. Once ICANN org has implemented a privacy/proxy service accreditation program, this recommendation once in effect replaces or otherwise supersedes EPDP phase 1 recommendation #14.
2. The intent of this recommendation is to provide clear instruction to registrars (and registries where applicable) that where a domain registration is done via accredited privacy/proxy provider, that data MUST NOT also be redacted. The working group is intending that domain registration data should NOT be both redacted and privacy/proxied.

Recommendation #20. City Field

The EPDP Team recommends that the EPDP Phase 1 recommendation is updated to state that redaction MAY be applied to the city field, instead of MUST.

Recommendation #21. Data Retention

The EPDP Team confirms its recommendation from phase 1 that 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). For clarity, this does not prevent Requestors, including ICANN Compliance, from requesting disclosure of these retained data elements for purposes other than TDRP, but disclosure of those will be subject to relevant data protection laws, e.g., does a lawful basis for disclosure exist. For the avoidance of doubt, this retention period does not restrict the ability of registries and registrars to retain data elements for longer periods.

Implementation Guidance:
For the avoidance of doubt, registrars are required to maintain the data for 15 months following the life of the registration and MAY delete that data following the 15-month period.

For clarity, this does not prevent the identification of additional retention periods for stated purposes by the controllers, as identified and as established by the controllers, for purposes other than TDRP; this does not exclude the potential disclosure of such retained data to any party, subject to relevant data protection laws.

Recommendation #22. Purpose 2
The EPDP Team recommends the following purpose be added to the EPDP Team Phase 1 purposes, which form the basis of the new ICANN policy:

- Contribute to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission.

3.7 EPDP Team Priority 2 Conclusions

Conclusion – OCTO Purpose
Having considered this input, most members of the EPDP Team agreed that at this stage, there is no need to propose an additional purpose(s) to facilitate ICANN's Office of the Chief Technology Officer (OCTO) in carrying out its mission. This reason for this agreement is because the newly updated ICANN Purpose 2 sufficiently covers the work of the OCTO, along with the work of other ICANN org teams such as Contractual Compliance and others. Most also agreed that the EPDP Team's decision to refrain from proposing an additional purpose(s) would not prevent ICANN org and/or the

community from identifying additional purposes to support unidentified future activities that may require access to non-public registration data.

Conclusion – Accuracy and WHOIS Accuracy Reporting System

Per the instructions from the GNSO Council, the EPDP Team will not consider this topic further; instead, the GNSO Council is expected to form a scoping team to further explore the issues in relation to accuracy and ARS to help inform a decision on appropriate next steps to address potential issues identified.

4 Next Steps

4.1 Next Steps

This Final Report will be submitted to the GNSO Council for its consideration and approval. 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.[53]
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

[53] 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[54] 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 policy recommendations for a System for Standardized Disclosure/Access will be agnostic to the modalities of the System.

[54] 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.

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 Intellectual Property 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".[55] 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

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

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.

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:

Member Type / Afiliation / Name	SOI	Start Date	Attended %	Role	Depart Date
Current Participant			86.0%		
Member					
ALAC (At-Large Advisory Committee)			93.2%		
Alan Greenberg	SOI	3-Apr-2019	93.2%		
Hadia El-Miniawi	SOI	3-Apr-2019	93.1%	LC	
BC (Commercial Business Users Constituency)			94.1%		
Margie Milam	SOI	3-Apr-2019	95.0%	LC	
Mark Svancarek	SOI	3-Apr-2019	93.2%		
GAC (Governmental Advisory Committee)			90.1%		
Christopher Lewis-Evans	SOI	15-May-2019	91.7%		
Georgios Tselentis	SOI	3-Apr-2019	87.7%		
Laureen Kappin	SOI	21-Oct-2019	91.1%	LC	
GNSO Council			96.6%		
Janis Karklins	SOI	18-Apr-2019	98.4%	Chair, LC	
Rafik Dammak	SOI	3-Apr-2019	94.8%	Liaison, LC	
ICANN (Internet Corporation for Assigned Names & Numbers)			89.4%		
Daniel Halloran		3-Apr-2019	84.2%	Liaison, LC	
Eleeza Agopian		6-Dec-2019	100.0%	Liaison	
ICANN Board			73.3%		
Becky Burr	SOI	9-Sep-2019	89.7%	Liaison, LC	
Chris Disspain	SOI	3-Apr-2019	64.9%	Liaison	
IPC (Intellectual Property Constituency)			88.0%		
Brian King	SOI	4-Aug-2019	85.0%	LC	
Franck Journoud	SOI	20-Jul-2019	100.0%		
ISPCP (Internet Service Providers and Connectivity Providers Constituency)			71.3%		
Fiona Asonga	SOI	3-Apr-2019	61.4%		
Thomas Rickert	SOI	3-Apr-2019	81.0%	LC	
NCSG (Non-Commercial Stakeholder Group)			75.0%		
Amr Elsadr	SOI	3-Apr-2019	55.2%		
Johan (Julf) Helsingius	SOI	3-Apr-2019	77.2%		
Milton Mueller	SOI	3-Apr-2019	71.4%		
Stefan Filipovic	SOI	21-May-2019	97.5%		
Stephanie Perrin	SOI	3-Apr-2019	80.7%	LC	
RrSG (Registrar Stakeholder Group)			82.8%		
James Bladel	SOI	3-Apr-2019	73.3%		
Matt Serlin	SOI	3-Apr-2019	87.7%		
Volker Greimann	SOI	16-Apr-2019	87.7%	LC	
RySG (Registry Stakeholder Group)			90.7%		
Alan Woods	SOI	3-Apr-2019	84.5%		
Marc Anderson	SOI	3-Apr-2019	95.1%		
Matthew Crossman	SOI	3-Apr-2019	93.0%	LC	
SSAC (Security and Stability Advisory Committee)			87.5%		
Ben Butler	SOI	3-Apr-2019	86.0%		
Tara Whalen	SOI	15-May-2019	89.4%	LC	

The Alternates of the EPDP Team are:

Member Type / Afiliation / Name	SOI	Start Date	Attended %	Role	Depart Date
Alternate					
ALAC (At-Large Advisory Committee)			33.3%		
Bastiaan Goslings	SOI	3-Apr-2019	42.9%		
Holly Raiche	SOI	3-Apr-2019	20.0%		
BC (Commercial Business Users Constituency)			97.6%		
Steve DelBianco	SOI	3-Apr-2019	97.6%		
GAC (Governmental Advisory Committee)			83.3%		
Olga Cavalli	SOI	22-May-2019	90.9%		
Rahul Gosain	SOI	3-Apr-2019	64.3%		
Ryan Carroll	SOI	18-Dec-2019	100.0%		
IPC (Intellectual Property Constituency)			95.7%		
Jennifer Gore	SOI	3-Apr-2019	95.7%		
ISPCP (Internet Service Providers and Connectivity Providers Constituency)			20.0%		
Suman Lal Pradhan	SOI	3-Apr-2019	20.0%		
NCSG (Non-Commercial Stakeholder Group)			75.0%		
David Cake	SOI	3-Apr-2019	78.6%		
Tatiana Tropina	SOI	3-Apr-2019	66.7%	LC	
RrSG (Registrar Stakeholder Group)			93.3%		
Owen Smigelski	SOI	16-Apr-2019	95.6%		
Sarah Wyld	SOI	3-Apr-2019	98.0%		
Theo Geurts	SOI	3-Apr-2019	50.0%		
RySG (Registry Stakeholder Group)			86.8%		
Arnaud Wittersheim	SOI	3-Apr-2019	69.2%		
Beth Bacon	SOI	22-Apr-2019	78.9%		
Sean Baseri	SOI	6-Nov-2019	97.2%		
SSAC (Security and Stability Advisory Committee)			63.9%		
Greg Aaron	SOI	5-Oct-2019	72.0%		
Rod Rasmussen	SOI	3-Apr-2019	27.3%		

Staff Support of the EPDP Team are:

Member Type / Afiliation / Name	SOI	Start Date	Attended %	Role	Depart Date
Staff Support					
ICANN (Internet Corporation for Assigned Names & Numbers)					
Caitlin Tubergen		3-Apr-2019		LC	
Marika Konings		3-Apr-2019			
Berry Cobb		3-Apr-2019			
Amy Bivens		3-Jun-2019		LC	
Terri Agnew		3-Apr-2019			
Andrea Glandon		3-Apr-2019			
Julie Bisland		20-Jun-2019			
Michelle DeSmyter		20-Jun-2019			
Nathalie Peregrine		3-Apr-2019			

The former Members of the EPDP Team are:

Member Type / Afiliation / Name	SOI	Start Date	Attended %	Role	Depart Date
Fomer Participant					
Member					
GAC (Governmental Advisory Committee)			70.7%		
Ashley Heineman	SOI	3-Apr-2019	70.7%		21-Oct-2019
ICANN (Internet Corporation for Assigned Names & Numbers)			77.4%		
Trang Nguyen		3-Apr-2019	77.4%	Liaison	10-Apr-2019
ICANN Board			80.0%		
Leon Felipe Sanchez Ambia	SOI	3-Apr-2019	80.0%	Liaison, LC	9-Sep-2019
IPC (Intellectual Property Constituency)			87.0%		
Alex Deacon	SOI	3-Apr-2019	87.0%		1-Dec-2019
NCSG (Non-Commercial Stakeholder Group)			65.1%		
Farzaneh Badiei	SOI	3-Apr-2019	65.1%		20-Dec-2019
Ayden Fabien Férdeline	SOI	3-Apr-2019	67.9%		20-Dec-2019
RySG (Registry Stakeholder Group)			70.6%		
Kristina Rosette	SOI	22-Apr-2019	80.0%	LC	7-Aug-2019

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/.

Annex D - Community Input

D.1. Request for SO/AC/SG/C 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.

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

D.2. Public Comment forum on the Initial Report

On 7 February 2020, the EPDP Team published its Initial Report for public comment. The Initial Report outlined the core issues discussed in relation to the proposed System for Standardized Access/Disclosure to non-public gTLD registration data ("SSAD") and accompanying preliminary recommendations.

The EPDP Team used a Google form to facilitate review of public comments. Forty-five contributions were received from GNSO Stakeholder Groups, Constituencies, ICANN Advisory Committees, companies and organizations, in addition to two contributions from individuals. The input provided is at: https://docs.google.com/spreadsheets/d/1EBiFCsWfqQnMxEcCaKQywCccEVdBc9_ktPA3PU8nrQk/edit?usp=sharing.

To facilitate its review of the public comments, the EPDP Team developed a set of public comment review tools (PCRTs) and discussion tables (see

https://community.icann.org/x/Hi6JBw). Through online review and plenary sessions, the EPDP Team completed its review and assessment of the input provided and agreed on changes to made to the recommendations and/or report.

D.3. Public Comment on the Addendum

On 26 March 2020, the EPDP Team published an Addendum to the Initial Report for public comment. The Addendum concerns the EPDP Team's preliminary recommendations and/or conclusions on the priority 2 items as listed above.

The EPDP Team used a Google form to facilitate review of public comments. Twenty-eight contributions were received from GNSO Stakeholder Groups, Constituencies, ICANN Advisory Committees, companies and organizations, in addition to one contribution from an individual. The input provided is at: https://docs.google.com/spreadsheets/d/1jN5ThNtmcVJ8txdAGw0ynl5vrGJOuEv8xeccvzjR9qM/edit#gid=2086811131.

To facilitate its review of the public comments, the EPDP Team developed a set of public comment review tools (PCRTs) and discussion tables (see https://community.icann.org/x/Hi6JBw). Through online review and plenary sessions, the EPDP Team completed its review and assessment of the input provided and agreed on which priority 2 recommendations and/or conclusions were ready to be included in this Final Report.

Annex E– 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?

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[56]

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

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

processor with instructions and terms of the contract", and efforts to instruct 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[57] (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)

[57] 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.

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 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

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 eliminate581 this risk?

c. In this scenario, would the CP be a controller or a processor592, 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?

[58] "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

[59] 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

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).[60]

- 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

[60] 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."

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

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.

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.

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).

Question 5 (Pseudonymized Email Addresses)

The group has discussed the option of replacing the email address provided by the data subject with an alternate email address that would in and of itself not identify the data subject (Example: 'sfjgsdfsafgkas@pseudo.nym'). With this approach, two options emerged in the discussion, where (a) the same unique string would be used for multiple registrations by the data subject ('pseudonymisation'), or (b) the string would be unique for each registration ('anonymization'). Under option (a), the identity of the data subject might - but need not necessarily - become identifiable by cross-referencing the content of all domain name registrations the string is used for.

From these options, the following question arose: Under options (a) and/or (b), would the alternate address have to be considered as personal data of the data subject under the GDPR and what would be the legal consequences and risks of this determination with regard to the proposed publication of this string in the publicly accessible part of the registration data service (RDS)?

Bird & Bird's Summary Answer

We think either option ((a) or (b)) would still be treated as the publication of personal data on the web. This would seem to be a case covered by a statement made in the Article 29 Working Party's 2014 Opinion on Anonymization techniques [ec.europa.eu]: "when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this data set (for example after removal or masking of identifiable data), the resulting data set is still personal data." The purpose for making this e-mail address available, even though it's masked, is presumably to allow third parties to directly contact the data subject (e.g. to serve them with court summons, demand takedowns, etc.) – so it's quite clearly linked to that particular data subject, at least so far as ICANN/Contracted Parties are concerned. However, either option would be seen as a valuable privacy-enhancing technology (OPET) / privacy by design measure.

Question 6 (Consent)

Registration data submitted by legal person registrants may contain the data of natural persons. A Phase 1 memo stated that registrars can rely on a registrant's self-identification as legal or natural person if risk is mitigated by taking further steps to ensure the accuracy of the registrant's designation. As a follow up to that memo: what are the consent options and requirements related to such designations? Specifically: are data controllers entitled to rely on a statement obligating legal person registrants to obtain consent from a natural person who would act as a contact and whose information may be publicly displayed in RDS? If so, what representations, if any, would be helpful for the controller to obtain from the legal person registrant in this case?

As part of your analysis please consult the GDPR policies and practices of the Internet protocol (IP address) registry RIPE-NCC (the registry for Europe, based in the Netherlands). RIPE-NCC's customers (registrants) are legal persons being displayed publicly in WHOIS. RIPE-NCC places the responsibility on its legal-person registrants to obtain permission from those natural persons, and provides procedures and safeguards for that. RIPE-NCC states mission justifications and data collection purposes similar to those in ICANN's Temporary Specification. Could similar policies and procedures be used at ICANN?

Also see the policies of ARIN, the IP address registry for North America. ARIN has some customers located in the EU. ARIN also publishes the data of natural persons in its WHOIS output. ARIN's customers are natural persons, who submit the data of natural person contacts.

Bird & Bird's Summary Answer

This document analyses the consent requirements set out in the GDPR and examines consents options for the purpose of publishing in RDS personal data provided in the context of the registration of legal person registrants.

Consent requirements

Pursuant to the GDPR, consent must be freely given, specific, informed and unambiguous. Also, it needs to be obtained prior to the processing taking place. Controllers must be able to demonstrate that valid consent has been given and individuals have the right to withdraw consent at any time. Under the GDPR, the obligation to obtain consent lies with the controller. The controller may instruct a third party to obtain consent from individuals on its behalf; however, doing so will not relieve the controller from its obligations under the GDPR.

Consent options

On the basis of the above requirements, this document examines the following options of obtaining consent for making personal data public in RDS and sets out the compliance considerations of each option:

1. Controllers seek valid consent directly from individuals
    - Making personal data public in RDS is optional.
    - Prior to making personal data public, the controller contacts individuals directly to seek consent in line with the GDPR.
    - In the event of refusal to consent or failure to respond, the personal data will not be made public

2. Registrant obtains valid consent and provides evidence to controller
    - Making personal data public in RDS is optional.
    - Prior to making personal data public, the controller requires the registrant to:(a) obtain individuals' consent; and (b) provide to the controller evidence that consent has been obtained.
    - In the event of refusal to consent or failure to receive evidence, the personal data will not be made public

3. Registrant obtains valid consent and controller confirms this with the individual
    - Prior to making personal data public, the controller requires the registrant to:(a) obtain individuals' consent; and (b) provide to the controller evidence that consent has been obtained.
    - Controller follows up with the individual directly: it informs them that the registrant has confirmed they have granted consent.

4. Registrant undertakes the obligation to obtain consent
    - Registrants are allowed to provide non-personal contact details.
    - Registration data is made public by default (irrespective of whether or not personal data is included).
    - By means of a statement, registrants undertake to ensure they have obtained individuals' consent if they choose to provide personal data.

Question 7 (Accuracy)

Question 1a

Who has standing to invoke the Accuracy Principle? We understand that a purpose of the Accuracy Principle is to protect the Data Subject from harm resulting from the processing of inaccurate information. Do others such as contracted parties and ICANN (as Controllers), law enforcement, IP rights holders, etc. have standing to invoke the Accuracy Principle under GDPR? In responding to this question, can you please clarify the parties/interests that we should consider in general, and specifically when interpreting the following passages from the prior memos:

- Both memos reference "relevant parties" in several sections. Are the "relevant parties" limited to the controller(s) or should we account for third-party interests as well?
    - "There may be questions as to whether it is sufficient for the RNH or Account Holder to confirm the accuracy of information relating to technical and administrative contacts, instead of asking information of such contacts directly. GDPR does not necessarily require that, in cases where the personal data must be validated, that it be validated by the data subject herself. ICANN and the relevant parties may rely on third-parties to confirm the accuracy of personal data if it is reasonable to do so. Therefore, we see no immediate reason to find that the current procedures are insufficient." (emphasis added) (Paragraph 19 – Accuracy)
    - "In sum, because compliance with the Accuracy Principle is based on a reasonableness standard, ICANN and the relevant parties will be better placed to evaluate whether these procedures are sufficient. From our vantage point, as the procedures do require affirmative steps that will help confirm accuracy, unless there is reason to believe these are insufficient, we see no clear requirement to review them." (emphasis added) (Paragraph 21-Accuracy)
    - "If the relevant parties had no reason to doubt the reliability of a registrant's self-identification, then they likely would be able to rely on the self-identification alone, without independent confirmation. However, we understand that the parties are concerned that some registrants will not understand the question and will wrongly self-identify. Therefore, there would be a risk of liability if the relevant parties did not take further steps to ensure the accuracy of the registrant's designation." (emphasis added) (Paragraph 17 –Legal v. Natural)

1.b Similarly, the Legal vs. Natural person memo refers to the "importance" of the data in determining the level of effort required to ensure accuracy. Is the assessment of the "importance" of the data limited to considering the importance to the data subject and the controller(s), or does it include the importance of the data to third-parties as well (in this case law enforcement, IP rights holders, and others who would request the data from the controller for their own purposes)?

- "As explained in the ICO guidance, "The more important it is that the personal data is accurate, the greater the effort you should put into ensuring its accuracy. So if you are using the data to make decisions that may significantly affect the individual concerned or others, you need to put more effort into ensuring accuracy." (Paragraph 14 –Legal vs. Natural)

Bird & Bird's Executive Summary

This document examines further considerations in relation to the Accuracy Principle (the parties with the obligation to comply with this principle, persons that have the standing to invoke it, and the basis on which data accuracy is to be assessed). It sets out the factors to be considered when assessing data accuracy and provides recommendations of measures to enhance the accuracy of registration data held by contracted parties.

Parties subject to Accuracy Principle and "relevant parties"

The obligation to comply with the GDPR's Accuracy Principle lies with the controller(s). References to "relevant parties" in the Accuracy and the Legal vs. Natural memos were to the relevant controller(s) of WHOIS data.

Parties having the right to invoke the Accuracy Principle

The GDPR provides for a range of remedies: complaints to supervisory authorities, judicial remedies and right to compensation from a controller or processor. Data subjects (and where allowed by national law, their representatives) have the right to exercise all remedies set forth in the GDPR. In some instances, these rights may also be exercised by other – natural or legal-persons, for example, those affected by the decision of a supervisory authority or those suffered damage as a result of an infringement of the GDPR.

Interests of various parties when considering accuracy

The purpose for which personal data is processed is relevant to determining the measures required to ensure data accuracy. The data subject's interests must be taken into account when assessing data accuracy. In some circumstances, the controller's interests will also be relevant. Although there are a few references to rights of "others" in ICO's accuracy guidance, this point is not illuminated further in our review of guidance, case law or literature. Given the lack of guidance, we do not recommend placing too much emphasis on this point.

Reasonable measures for data accuracy

The Accuracy Principle has not been extensively examined in literature and case law and references to it are limited. The reasonable and appropriate character of accuracy measures should be considered in the light of the GDPR's risk-based approach, taking into account,

among other things, the purpose and impact of processing. A list of suggested accuracy measures is set out in this document.

Question 8 (Automation Use Cases)

Background

1. Under the first scenario, the automation would be carried out within a Central Gateway tasked with receiving requests from accredited users. The Central Gateway would make an automated recommendation on whether or not the requested data should be disclosed whilst the ultimate decision of disclosing data would rest with the Contracted Parties, which could either follow the recommendation or not (Scenario 1.a.). Contracted Parties with enough confidence in the Gateway may choose to automate the decision to disclose the data (Scenario 1.b.).

2. Under the second scenario, the decision to disclose the registrant data would be taken by the Central Gateway without the Contracted Party being able to review the request. The Central Gateway would take this decision either (i) after obtaining the relevant data from the Contracted Party and evaluating the data as part of its decision-making (Scenario 2.a.), or (ii) without obtaining the registrant data (in which case, the decision would be based solely on information about the Requestor and the assertions made in the request) (Scenario 2.b.). One example given of the latter scenario would be automated disclosure of registration data for microsoft-login.com to the verified owner of the trademark MICROSOFT, in response to a request alleging trademark infringement and asserting intent to process the data for the establishment, exercise or defence of legal claims. We have been asked to assume that each scenario would be subject to a set of safeguards which are included in this memo as Appendix 1.

A. Use cases under Scenario 1:

In light of the advice previously provided in the memos on Question 1&2 (Liability) and Question 3 (Automation), please provide the following analysis for each use case in Exhibit 1:

1. Please describe the risk of liability for the Central Gateway and Contracted Parties ("CPs") related to automating this recommendation, and to automating the decision to disclose personal information to a third-party. If there is additional information required to assess the risk, please note the additional information needed.

2. Is the decision to disclose personal information to a third-party a decision "which produces legal effects concerning [the data subject] or similarly significantly affects him or her" within the scope of Article 22?

3. Are there additional measures or safeguards that would mitigate the risk of liability?

4. Does automated decision-making performed in this manner impact your analysis on the roles/liability of the parties described in the Question 1&2 memo (e.g., Contracted Parties

remain controllers with liability where “disclosure takes place in an automated fashion, without any manual intervention.” 1.1.4).

B. Use cases under Scenario 2:

In the second -alternative- scenario, where the Central Gateway has the contractual ability to require the Contracted Parties to provide the data to the Central Gateway:

1. How do the alternative scenarios impact the analysis provided in Questions 1 through 4 above?

2. Which scenario involves the least risk of liability for Contracted Parties? In responding to this, please state your assumptions regarding the respective roles of ICANN and contracted parties, including a scenario where the Centralized Gateway has outsourced decision making to an independent legal service provider.

C. Additional automation clarifications

1. If the decision to disclose personal data to a third party is automated, in what manner must the Controller(s) provide the registrant with information concerning the possibility of automated decision-making in processing of his or her personal information? How should this information be communicated to the registrant, and what information pertaining to the automated decision-making must be communicated to the registrant in order to ensure fair and transparent processing pursuant to Article 13?

2. Does the provision of the information in the answer to question C.1 above by the Controller(s) affect the registrant’s right to obtain confirmation as to whether or not automated decision-making to disclose their personal information to a third-party has taken place? Does it affect the registrant’s right to obtain associated meaningful information as per Article 15.1(h)?

3. Does the manner in which the decision making is performed above impact the way in which this information must be provided?

4. What role does proximate cause play in determining whether a decision to disclose produces a legal or similarly significant effect (i.e. how related must the decision to disclose a registrant’s personal data be to the ultimate legal or similarly significant effect of personal data processing)? Please describe the risk of liability to the Central Gateway or Contracted Party if, after receiving personal data, the Requestor engages in its own processing which has a legal or similarly significant effect.

5. In Section 1.12 in the previous memo on Automation, Bird & Bird stated: It may also be possible to structure the SSAD so that it does not involve "a decision based solely on automated processing". To expand, rather than the SSAD requesting information from requesters and

evaluating if the relevant criteria for release of non-public registration data are met, the SSAD could publish the categories of requests which will be accepted and ask Requestors to confirm that they meet the relevant criteria. In this case, there would be no automated processing leading to a decision to release the data. The SSAD could 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. Could you please elaborate on how (i) publishing the categories of requests that will be approved and (ii) requiring a Requestor to manually select the applicable category and confirm that they meet the criteria for that category of requests would make the decision to disclose "not automated"?

Bird & Bird's Executive Summary

This document examines the scenarios and use cases presented by the EPDP Team in relation to automated decisions for disclosure of non-public registrant data. It identifies the cases of fully automated decisions that would fall under the scope of Art. 22 GDPR, challenges associated with Art. 22 and available alternatives. The document further suggests data protection safeguards and examines transparency considerations in the SSAD context. Finally, it examines the status of the parties under each scenario and the associated risk of liability.

Art. 22 decisions and alternatives

Art. 22 GDPR applies to fully automated decisions which produce legal or similarly significant effects. Art. 22 decisions are only allowed in limited cases, which are not likely to apply to the SSAD context. Fully automated decisions will only be allowed if they: (a) do not include the processing of personal data; (b)do not produce legal or similarly significant effects; (c) are authorised by applicable EU or Member State law which lays down suitable measures to protect individuals; or (d) are covered by a national derogation from Art. 22 (for example, for the purpose of detection of criminal offences). In all other cases, there needs to be meaningful human involvement in the decision making process.

Do Art. 22 criteria apply to SSAD?

(a) Solely automated processing: For Art. 22 to apply, there needs to be some processing of personal data, but there is no requirement that only personal data is processed for the decision. The decision examined here will in most cases involve the processing of personal data – this will be the case irrespective of whether or not the Central Gateway has access to the requested data and takes account of such data in the decision making. Apart from Scenario 1.a where the SSAD would only issue an automated recommendation, all other scenarios would include a decision (to disclose registrant data to third parties) based solely on automated processing.

(b) Legal or similarly significant effect: the term is not defined in the GDPR; however, it indicates an elevated threshold. Whether or not the disclosure of registrant data has such an

effect, will depend on the circumstances of the request: the document assesses the nature of the effects of disclosure under each use case. We have given clear yes and no answers where possible: some use cases would benefit from further discussion. The role of proximate cause in determining the effects of a decision has not been examined by courts or supervisory authorities. There is some discussion in German literature; however, given the lack of wider discussion, the views of supervisory authorities on this topic could be useful, as this may permit automation of the SSAD on the basis that the Central Gateway/CPs are only taking a preparatory decision.

Safeguards

A list of suggested data protection safeguards is set out in Appendix 2 of this document. This includes among other things: engaging with supervisory authorities, clearly scoping each use case and establishing a legal basis, imposing appropriate terms of disclosure on the Requestor, implementing appropriate security measures, taking measures to comply with the accountability principle, establishing policies for satisfying individuals' rights, and entering into appropriate data protection clauses with processors.

Transparency

The manner of providing information is not affected by the existence of automated decision making; but the content of the information is.

- The information will typically be provided through the privacy notice; given the importance of the SSAD in the Domain Name system, it would be appropriate to present it in a prominent manner.
- It would be most efficient for registrars to provide the relevant information (given their direct relationship with registrants), irrespective of whether not they are considered controllers in the SSAD context. If they are not controllers, but provide the information on behalf of the controller, this should be made clear to registrants.
- In terms of the content, for Art. 22 decisions only, the notice must also include information about: the existence of automated decision, the logic involved and the significance and envisaged consequences of the processing.
- The elements of Art. 15 GDPR (right of access) need to be provided on request even if they have already been included in the notice.
- The right of access requires controllers to provide information on the recipients to whom the data "have been or will be disclosed": this indicates that, absent applicable exemptions, registrants exercising their right of access must be informed about disclosures of their data to third parties.

Status of parties

(a) Under Scenario 1, the ultimate decision to disclose registrant data rests with the CPs. The analysis carried out in the Liability memo would also apply here and most likely CPs would be considered by supervisory authorities as joint controllers along with ICANN.

(b) Under Scenario 2, the situation is less clear. Depending on whether a macro-or micro-level approach is adopted, the CPs may be found to be (joint) controllers for the automated decision making and the disclosure of data to Requestors or merely for the disclosure of data to the Central Gateway. We think the second option (controllers just for the disclosure of data to the Central Gateway) is the better analysis, but the point is not clear. The outsourcing of the decision making to an independent legal service provider would be unlikely to alter the above position.

In both scenarios, it would not be plausible to argue that CPs are processors.

Liability of CPs is examined in respect of:

(a) status of CPs: where CPs are joint controllers, it is important to clearly allocate tasks and responsibilities by means of an agreement;
(b) type of liability:

- Liability towards individuals: the rule is joint and several liability and CPs can be held liable for the entire damage caused by processing they are involved in, irrespective of their status. They can only avoid this by demonstrating that they were not in any way involved in the event giving rise to the damage. Otherwise, they have the right to claim back from the other controllers the part of compensation corresponding to their responsibility.
- Liability to supervisory authorities: joint and several liability is less clear here and there is scope to argue that enforcement action should be imposed based on the "degree of responsibility" of the party.

In terms of risk, Scenario 2 seems to present lower risk of liability both in respect of compensation to individuals and of enforcement action by supervisory authorities.