

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

[Date]

Status of This Document

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

Preamble

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

Table of Contents

1	<u>EXECUTIVE SUMMARY</u>	3
1.1	CONCLUSIONS AND NEXT STEPS	4
1.2	OTHER RELEVANT SECTIONS OF THIS REPORT	4
2	<u>EPDP TEAM APPROACH</u>	5
2.1	WORKING METHODOLOGY	5
2.2	MIND MAP, WORKSHEETS AND BUILDING BLOCKS	5
2.3	PRIORITY 1 AND PRIORITY 2 TOPICS	6
2.4	LEGAL COMMITTEE	7
2.5	CHARTER QUESTIONS	7
3	<u>EPDP TEAM RESPONSES TO CHARTER QUESTIONS & PRELIMINARY RECOMMENDATIONS</u>	8
3.1	SYSTEM FOR STANDARDIZED ACCESS/DISCLOSURE TO NON-PUBLIC REGISTRATION DATA (SSAD)	8
3.2	ICANN BOARD AND ICANN ORG INPUT	12
3.3	SSAD UNDERLYING ASSUMPTIONS	12
3.4	CONVENTIONS USED IN THIS DOCUMENT	13
3.5	EPDP TEAM PRELIMINARY RECOMMENDATIONS	13
4	<u>NEXT STEPS</u>	44
4.1	NEXT STEPS	44
	<u>GLOSSARY</u>	45
	<u>ANNEX A – SYSTEM FOR STANDARDIZED ACCESS/DISCLOSURE TO NON-PUBLIC REGISTRATION DATA – BACKGROUND INFO</u>	51
	<u>ANNEX B – GENERAL BACKGROUND</u>	83
	<u>ANNEX C – EPDP TEAM MEMBERSHIP AND ATTENDANCE</u>	85
	<u>ANNEX D - COMMUNITY INPUT</u>	88
	<u>ANNEX E - BALANCING TEST FRAMEWORK</u>	89
	<u>ANNEX F – LEGAL COMMITTEE</u>	88

1 Executive Summary

2 1.1 Background

3
4 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.

11
12 On 19 July 2018, the GNSO Council [initiated](#) an Expedited Policy Development Process (EPDP) and [chartered](#) the EPDP on the Temporary Specification for gTLD Registration Data team. In accordance with the Charter, EPDP team membership was expressly limited. However, all ICANN Stakeholder Groups, Constituencies and Supporting Organisations interested in participating are represented on the EPDP Team.

17
18 During phase 1 of its work, the EPDP Team was tasked to determine if the Temporary Specification for gTLD Registration Data should become an ICANN Consensus Policy as is, or with modifications. This Initial Report concerns phase 2 of the EPDP Team’s charter which covers: (i) discussion of a system for standardized access/disclosure to nonpublic registration data, (ii) issues noted in the [Annex to the Temporary Specification for gTLD Registration Data](#) (“Important Issues for Further Community Action”), and (iii) outstanding issues deferred from Phase 1, e.g., legal vs. natural persons, redaction of city field, et. al. For further details, please see [here](#).

26
27 The EPDP Team will not finalize its responses to the charter questions and recommendations to the GNSO Council until it has conducted a thorough review of the comments received during the public comment period on this Initial Report. At this time, no formal consensus call has been taken on these responses and preliminary recommendations, but this Initial Report did receive the support of the EPDP Team for publication for public comment.² Where applicable, the Initial Report indicates where positions within the Team differ.

34
35 Notwithstanding the above, the EPDP Team is putting forward the following preliminary recommendations and related questions for community consideration:

37
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/>.

² Following a review of public comments, the EPDP Team will take a formal consensus call before producing its Final Report.

38 [To be updated following final review]

39

40 As a result of external dependencies and time constraints, this Initial Report does not
41 include priority 2 items. Priority 2 items are detailed on pp. 6-7 of this Report. Once
42 addressed, these are expected to be published in a separate Initial Report.

43

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

51 1.2 Conclusions and Next Steps

52

53 This Initial Report will be posted for public comment for 45 days. After the EPDP Team's
54 review of public comments received on this Report, the EPDP Team will update and
55 finalize this Report as deemed necessary for submission to the GNSO Council.

56 1.3 Other Relevant Sections of this Report

57

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

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

67

68

2 EPDP Team Approach

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

2.1 Working Methodology

76
77 The EPDP Team began its deliberations for phase 2 on 2 May 2019. The Team agreed to
78 continue its work primarily through conference calls scheduled one or more times per
79 week, in addition to email exchanges on its mailing list. Additionally, the EPDP Team
80 held four face-to-face meetings: the first set of face-to-face discussions took place at
81 the ICANN65 Public Meeting in Marrakech, Morocco, two dedicated set of face-to-face
82 meetings, the second and fourth meeting, were held at the ICANN headquarters in Los
83 Angeles (LA) in September 2019 and January 2020, and the third face-to-face discussion
84 took place at the ICANN66 Public Meeting in Montreal, Canada. All of the EPDP Team’s
85 meetings are documented on its wiki [workspace](#), including its [mailing list](#), draft
86 documents, background materials, and input received from ICANN’s Supporting
87 Organizations and Advisory Committees, including the GNSO’s Stakeholder Groups and
88 Constituencies.

89
90 The EPDP Team also prepared a [Work Plan](#), which was reviewed and updated on a
91 regular basis. In order to facilitate its work, the EPDP Team used a template to tabulate
92 all input received in response to its request for Constituency and Stakeholder Group
93 statements (see Annex B). This template was also used to record input from other
94 ICANN Supporting Organizations and Advisory Committees and can be found in Annex
95 C.

96
97 The EPDP Team held a [community session](#) at the ICANN66 Public Meeting in Montreal,
98 during which it presented its methodologies and preliminary findings to the broader
99 ICANN community for discussion and feedback.

2.2 Mind Map, Worksheets and Building Blocks

101
102 In order to ensure a common understanding of the topics to be addressed as part of its
103 phase 2 deliberations, the EPDP Team mapped the topics using the following mind
104 maps, which allowed for the regrouping and consolidation of topics (see [mind map](#)).
105 This formed the basis for the subsequent development of the priority 1 and priority 2
106 worksheets (see [worksheets](#)) which the EPDP Team used to capture:

- 107 ● Issue description / related charter questions
- 108 ● Expected deliverable

- 109 ● Required reading
- 110 ● Briefings to be provided
- 111 ● Legal questions
- 112 ● Dependencies
- 113 ● Proposed timing and approach

114

115 The EPDP Team Chair also put forward a number of working definitions to ensure
116 consistent terminology and a shared understanding of terms used during the EPDP
117 Team’s deliberations (see [working definitions](#)).

118

119 Following the review of a number of real life [use cases](#), the EPDP Team established a
120 set of building blocks that the System for Standardized Access/Disclosure (“SSAD”)
121 would consist of, recognizing that a decision on the roles and responsibilities of the
122 different parties involved may be influenced by both legal advice and guidance from
123 the European Data Protection Board (“EDPB”).

124

125 2.3 Priority 1 and Priority 2 Topics

126

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

130

- 131 ● Display of information of affiliated vs. accredited privacy / proxy providers
- 132 ● Legal vs. natural persons
- 133 ● City field redaction
- 134 ● Data retention
- 135 ● Potential Office of the Chief Technology Officer Purpose
- 136 ● Feasibility of unique contacts to have a uniform anonymized email address
- 137
- 138 ● Accuracy and WHOIS Accuracy Reporting System

139

140 The EPDP Team agreed that priority should be given to completing the deliberations for
141 priority 1 items. It agreed, however, that where feasible, the Team would also
142 endeavor to make progress on priority 2 items in parallel. Although some discussions
143 have taken place in parallel, no priority 2 items have been addressed in this Initial
144 Report. The EPDP Team expects to turn its attention to these as soon as possible but
145 anticipates that priority 2 items will have their own Initial and Final Report, unless
146 some of the issues can be fast-tracked to align with the priority 1 topics addressed in
147 this Initial Report.

148

149

150 2.4 Legal Committee

151

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

157

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

160

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

167

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

170

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

174 2.5 Charter Questions

175

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

181

182

183 3 EPDP Team Responses to Charter Questions & 184 Preliminary Recommendations

185

186 The EPDP Team will not finalize its responses to the charter questions and
187 recommendations to the GNSO Council until it has conducted a thorough review of the
188 comments received during the public comment period on this Initial Report.
189 Additionally, if ICANN Org receives further guidance from the European Data Protection
190 Board (“EDPB”), the EPDP Team will consider this guidance in its Final Report.³ At the
191 time of publication of this Report, no formal consensus call has been taken on these
192 responses and preliminary recommendations; however, this Initial Report did receive
193 the support of the EPDP Team for publication for public comment.⁴ Where applicable,
194 differing positions have been reflected in the Report.

195

196 Note: During Phase 1 of the EPDP Team’s work, the EPDP Team was tasked with
197 reviewing the Temporary Specification. The [Temporary Specification](#) was established as
198 a response to the GDPR.⁵ Accordingly, the GDPR is the only law that is specifically
199 referenced in this report. The EPDP team has extensively deliberated whether this
200 Initial Report could be drafted in a way that is agnostic to any specific law, but the EPDP
201 Team determined that the report would benefit from explicit references to facilitate
202 the implementation of the Team’s recommendations. The GDPR is a regional law
203 covering multiple jurisdictions and - given the strict criteria it contains - compliance
204 with this law has a high probability of being compliant with other national data
205 protection laws. The EPDP team fully endorses ICANN’s aspiration to be globally
206 inclusive, and nothing in this report shall overturn the basic principle that
207 contracted parties can and must comply with locally applicable statutory laws and
208 regulations.

209 3.1 System for Standardized Access/Disclosure to Non-Public 210 Registration Data (SSAD)

211

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

215

³ See <https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-stevens-25oct19-en.pdf> and
<https://www.icann.org/en/system/files/files/unified-access-model-gtld-registration-data-25oct19-en.pdf>

⁴ Following a review of public comments, the EPDP Team will take a formal consensus call before producing its Final Report.

⁵ “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.”

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

219

- 220 • Full automation⁶ of the SSAD may not be possible, but the EPDP Team
221 recommends that the SSAD must be automated where technically feasible AND
222 legally permissible. Additionally, in areas where automation is not both
223 technically feasible and legally permissible, harmonization is the baseline
224 objective.
- 225 • Experience gained over time with SSAD disclosure requests and responses must
226 inform further streamlining and standardization of responses.
- 227 • In recognition of the expected evolving nature of SSAD and in an effort to avoid
228 having to conduct a PDP every time a change needs to be made, a feedback
229 mechanism, which focuses solely on the implementation of the SSAD and does
230 not contradict ICANN Bylaws, GNSO PDP Procedures and Guidelines, and/or
231 contractual requirements would need to be put in place to oversee and guide
232 the continuous improvements of the SSAD.
- 233 • SLAs need to be put in place, but these may need to be of an evolutionary
234 nature to recognize that there will be a learning curve.
- 235 • Responses to disclosure requests, regardless of whether review is conducted
236 manually or an automated responses is triggered, are returned from the
237 relevant Contracted Party directly to the requestor, but appropriate logging
238 mechanisms must be in place to allow for the SSAD to confirm that SLAs are
239 met and responses are being processed according to the policy (for example,
240 the Central Gateway MUST be notified when disclosure requests are rejected or
241 granted).

242 The benefits of this model are:

243

244 **Single location to submit requests**

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

253 **Standardized request forms**

- 254 ○ Reduces the number of disclosure requests that are denied due to
255 insufficient information

⁶ See Automation Preliminary Recommendation for further details.

- 256 ○ Increases the efficiency with which disclosing entities can review
257 requests
258 ○ Reduces uncertainty for requesters who now have a standard/uniform
259 set of data to provide when submitting disclosure requests.
260 ○ Reduces the need for individual set of required information by disclosing
261 parties

262 **Built-in authentication process**

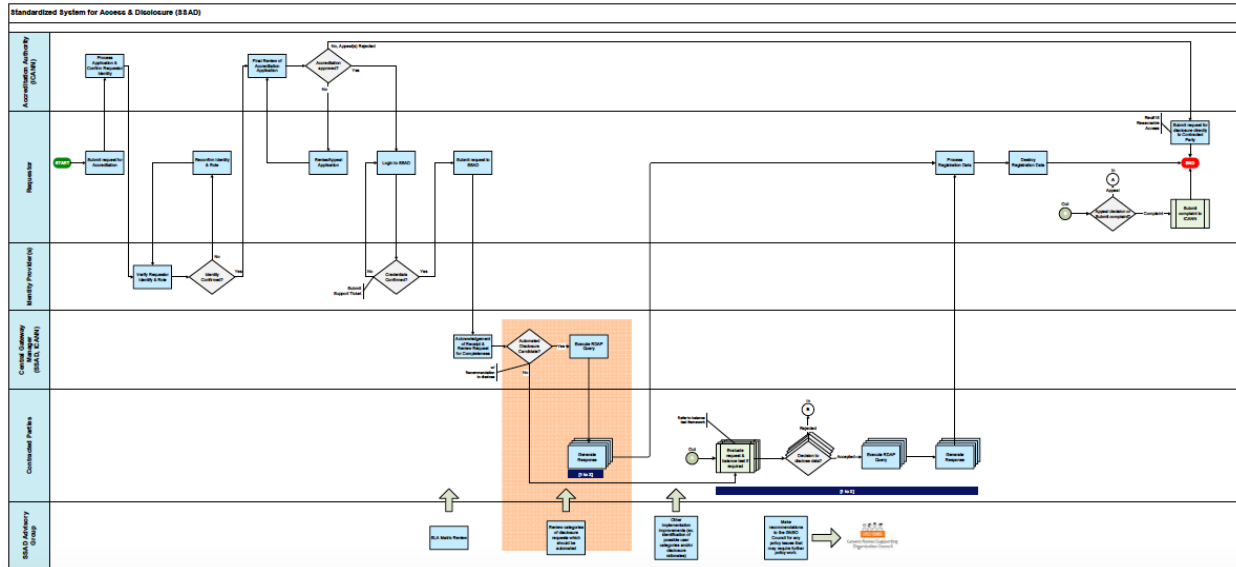
- 263 ○ Speeds up the review process for disclosing entities as they will not need
264 to re-verify the requestor
265 ○ External assurance that requestors have been verified can increase the
266 likelihood and/or speed of disclosure

267 **4. Standardized review and response process**

- 268 ○ Allows creation of a common response format
269 ○ Allows creation of rules, guidelines and best practices disclosing parties
270 can follow in reviewing and responding to requests
271 ○ Allows adoption of common response review system
272 ○ Allows automation of certain yet-to-be-defined requests by yet-to-be-
273 defined requestors
274 ○ Facilitates automated disclosure decision making in some scenarios
275 ○ The logging of requests and responses also allows ICANN Compliance to
276 audit the actions of disclosing entities, identifying any instances of
277 systemic non-compliance, and take appropriate enforcement action

278 This model has been visually represented hereunder;⁷ the diagram highlights which
279 aspects of the roles and responsibilities are expected to change depending on the
280 chosen model.
281

⁷ For a standalone version, please see https://community.icann.org/download/attachments/124847621/Visio-epdp-p2_swimlane_v0.5.pdf?version=1&modificationDate=1580312983428&api=v2. Please note that this is a visual representation of the policy recommendations, not policy in itself. For the sake of readability, not all aspects may be represented in this graphic. In case of conflict, the policy recommendations are the authoritative source.



282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308

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 Mechanism for the continuous evolution of SSAD. Responsible for collecting data on 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. For the purpose of the SSAD, the Identity Provider may be the Accreditation Authority itself or it may rely on zero or more 3rd parties.
- **Contracted Parties** – Responsible for responding to disclosure requests that do not meet the criteria for an automated response⁸.
- **Mechanism for the continuous evolution of SSAD** – Mechanism representative of the ICANN community responsible for 1) SLA matrix review; 2) provide guidance on which categories of disclosure requests should be automated; 3) other implementation improvements such as the identification of possible user

⁸ 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. The EPDP Team will further consider what these circumstances could be.

309 categories and/or disclosure rationales. The Mechanism may also make
310 recommendations to the GNSO Council for any policy issues that may require
311 further policy work.

312

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

315

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

318 3.2 ICANN Board and ICANN Org Input

319

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

325

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

333

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

344

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

349 3.3 SSAD Underlying Assumptions

350

351 The EPDP Team used the underlying assumptions outlined below to develop its
352 preliminary policy recommendations. These underlying assumptions do not necessarily
353 create new requirements for contracted parties; instead, the assumptions are designed
354 to assist both the readers of this Initial Report and the ultimate policy implementers in
355 understanding the intent and underlying assumptions of the EPDP Team in putting
356 forward the SSAD model and related recommendations. These assumptions may have
357 evolved by the time the EPDP Team publishes its Final Report; however, the EPDP
358 Team will note any changed assumptions in its Final Report.

359

- 360 ● The objective of the SSAD is to provide a predictable, transparent, efficient and
361 accountable mechanism for the access/disclosure of non-public registration
362 data.
- 363 ● The SSAD must be compliant with the GDPR and other applicable data
364 protection legislations for all parties.
- 365 ● SSAD must have the ability to adhere to these policy principles and
366 recommendations.
- 367 ● Given the decisions made by the EPDP team regarding the SSAD model, the
368 working assumption is that ICANN and Contracted Parties will be Joint
369 Controllers. This designation is based on a factual analysis of the policy as is
370 proposed.

371 3.4 Conventions Used in this Document

372 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD",
373 "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL"
374 in this document are to be interpreted as described in BCP 148 [RFC21199]
375 [RFC817410].

376

377 Note: Noting the EPDP team's choice of model, and pending the specific legal advice as
378 to the responsibility of the parties, and the identification as to the controllership of the
379 data, as it applies to the proposed model, the EPDP team notes that certain
380 statements, throughout the recommendations, may require refinement from
381 mandatory to permissive and vice versa. (e.g. 'Shall' to 'should', 'Must' to 'May' etc.).

382 3.5 EPDP Team Preliminary Recommendations

383

384 Preliminary Recommendation #1. Accreditation⁹

385

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

387

- 388 ● **Accreditation** - An administrative action by which the accreditation authority
389 declares that a user is approved to gain access to SSAD in a particular security
390 configuration with a prescribed set of safeguards.

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

- 391
- 392
- 393
- 394
- 395
- 396
- 397
- 398
- 399
- 400
- 401
- 402
- 403
- 404
- 405
- 406
- 407
- 408
- 409
- 410
- 411
- 412
- 413
- 414
- 415
- 416
- 417
- 418
- 419
- 420
- 421
- 422
- 423
- 424
- 425
- 426
- 427
- 428
- 429
- 430
- 431
- 432
- 433
- 434
- **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** - Independent entity that is contracted by ICANN org, or function that is carried out by ICANN Org itself if the Accreditation Authority function is outsourced to a third party, to carry out auditing requirements as outlined in auditing preliminary recommendation.
 - **Authentication** - The process or action of Validating the Identity Credential and Signed Assertions of a Requestor.
 - **Authorization** - A process for approving or denying disclosure non-public registration data.
 - **Credential**
 - **“Identifier Credential”**: A data object that is a portable representation of the association between an identifier and a unit of authentication information, and that can be presented for use in Validating an identity claimed by an entity that attempts to access a system. Example: [Username/Password], [OpenID credential], X.509 public-key certificate.
 - **“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.
 - **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.
 - **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 it may rely on zero or more 3rd parties.
 - **Revocation of User Credentials**- The event that occurs when an Identity Provider declares that a previously valid credential has become invalid.
 - **Validate** - To test or prove the soundness or correctness of a construct. (Example: The Discloser will Validate the Identity Credential and Signed Assertions as part of its Authorization process.)
 - **Validation** - Establish the soundness or correctness of a construct.
 - **Verify** - To test or prove the truth or accuracy of a fact or value. (Example: Identity Providers Verify the identity of the requestor prior to issuing an Identity Credential.)
 - **Verification** - The process of examining information to establish the truth of a claimed fact or value.
-

435

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

438

439 The following principles underpin the accreditation policy:

440

a) SSAD must only accept requests for access/disclosure from accredited
441 organizations or individuals. However, accreditation requirements must
442 accommodate any intended user of the system, including an individual or
443 organization who makes a single request. The accreditation requirements for
444 regular users of the system and a one-time user of the system may differ.

445

b) Both legal persons and/or individuals are eligible for accreditation. An individual
446 accessing SSAD using the credentials of an accredited entity warrants that the
447 individual is acting on the authority of the accredited entity.¹⁰

448

c) The accreditation policy defines a single Accreditation Authority, run and
449 managed by ICANN org. This Accreditation Authority may work with external or
450 third-party Identity Providers that could serve as clearinghouses to Verify
451 identity and authorization information associated with those requesting
452 accreditation.

453

d) The decision to authorize disclosure of registration data, based on Validation of
454 the Identity Credential, Signed Assertions, and data as required in preliminary
455 recommendation concerning criteria and content of requests, will reside with
456 the Registrar, Registry or ICANN, as applicable.

457

458 Requirements

459

e) Verifying the Identity of the Requestor: The Accreditation Authority MUST
460 verify the identity of the requestor, resulting in an Identity Credential.

461

f) Management of Signed Assertions: The Accreditation Authority MUST verify and
462 manage a set of dynamic assertions/claims associated with and bound to the
463 Identity Credential of the requestor. This verification, performed by an Identity
464 Provider, results in Signed Assertion.

465

g) Signed Assertions convey information such as:

466

○ Assertion as to the purpose(s) of the request

467

○ Assertion as to the legal basis of the requestor

468

○ Assertion that the user identified by the Identity Credential is affiliated
469 with the Accreditation Authority

470

○ Assertion regarding compliance with laws (e.g., storage, protection and
471 retention/disposal of data)

472

○ Assertion regarding agreement to use the disclosed data for the
473 legitimate and lawful purposes stated

474

○ Assertion regarding adherence to safeguards and/or terms of service
475 and to be subject to revocation if they are found to be in violation

¹⁰ Implementation guidance: The accredited entity is expected to develop appropriate policies and procedures to ensure appropriate use by an individual of its credentials.

- 476 ○ Assertions regarding prevention of abuse, auditing requirements,
477 dispute resolution and complaints process, etc.
- 478 ○ Assertions specific to the requestor – trademark ownership/registration
479 for example
- 480 ○ Power of Attorney statements, when/if applicable.
- 481 h) Validation of Identity Credentials and Signed Assertion, in addition to the
482 information contained in the request, facilitate the decision of the authorization
483 provider to accept or reject the Authorization of an SSAD request. For the
484 avoidance of doubt, the presence of these credentials alone DOES NOT result in
485 or mandate an automatic access / disclosure authorization. However, the ability
486 to automate access/disclosure authorization decision making is possible under
487 certain circumstances where lawful.
- 488 i) Defines a base line “code of conduct” that establishes a set of rules that
489 contribute to the proper application of data protection laws - including the
490 GDPR - for the ICANN community, including:
- 491 ○ A clear and concise explanatory statement.
- 492 ○ A defined scope that determines the processing operations covered (the
493 focus for SSAD would be on the Disclosure operation.)
- 494 ○ Mechanism that allow for the monitoring of compliance with the
495 provisions.
- 496 ○ Identification of an Accreditation Body Auditor (a.k.a. monitoring body)
497 and definition of mechanism(s) which enable that body to carry out its
498 functions.
- 499 ○ Description as to the extent a “consultation” with stakeholders has been
500 carried out.
- 501 ○ Etc.
- 502
- 503 The accreditation authority:
- 504 j) MUST have a uniform baseline application procedure and accompanying
505 requirements for all applicants requesting accreditation, including:
- 506 ○ Definition eligibility requirements for accredited users
- 507 ○ Identity Validation, Procedures
- 508 ○ Identity Credential Management Policies: lifetime/expiration, renewal
509 frequency, security properties (password or key policies/strength), etc.
- 510 ○ Identity Credential Revocation Procedures: circumstances for
511 revocation, revocation mechanism(s), etc. [see also “Accredited User
512 Revocation & abuse section below]
- 513 ○ Signed Assertions Management: lifetime/expiration, renewal frequency,
514 etc.
- 515 ○ NOTE: requirements beyond the baseline listed above may be necessary
516 for certain classes of requestors.
- 517 k) MUST define a dispute resolution and complaints process to challenge actions
518 taken by the Accreditation Authority.

- 519 l) MUST be audited by an auditor on a regular basis. Should the Accreditation
520 Authority be found in breach of the accreditation policy and requirements, it
521 will be given an opportunity to address the breach, but in cases of repeated
522 failure, a new Accreditation Authority must be identified or created.
523 Additionally, accredited entities MUST be audited for compliance with the
524 accreditation policy and requirements on a regular basis; (Note: detailed
525 information regarding auditing requirements can be found in the Auditing
526 preliminary recommendation).
- 527 m) MAY develop user groups / categories to facilitate the accreditation process as
528 all requestors will need to be accredited, and accreditation will include identity
529 verification.
- 530 n) MUST report publicly and on a regular basis on the number of accreditation
531 requests received, accreditation requests approved/renewed, accreditations
532 denied, accreditations revoked, complaints received and information about the
533 identity providers it is working with.
534

535 Accredited User Revocation & Abuse:

- 536 o) Revocation, within the context of the SSAD, means the Accreditation Authority
537 can revoke the accredited user's status as an accredited user of the SSAD. A
538 non-exhaustive list of examples where revocation may apply include 1) the
539 accredited user's violation of the code of conduct, 2) the accredited user's
540 abuse of the system, 3) a change in affiliation of the accredited user, or 4)
541 where prerequisites for accreditation no longer exist.
- 542 p) A mechanism to report abuse committed by an accredited user must be
543 provided by SSAD. Reports must be relayed to the Accreditation Authority for
544 handling.
- 545 q) The revocation policy for individuals/entities should include graduated
546 penalties. In other words, not every violation of the system will result in
547 Revocation; however, Revocation may occur if the Accreditation Authority
548 determines that the accredited individual or entity has materially breached the
549 conditions of its accreditation and failed to cure based on: a) a third-party
550 verified complaint received; b) results of an audit or investigation by the
551 Accreditation Authority or auditor; c) any misuse or abuse of privileges
552 afforded; d) repeated violations of the accreditation policy; e) results of audit or
553 investigation by a DPA.
- 554 r) In the event there is a pattern or practice of abusive behavior within an entity,
555 the credential for the entity could be suspended or revoked as part of a
556 graduated sanction.
- 557 s) Revocation will prevent re-accreditation in the future absent special
558 circumstances presented to the satisfaction of the Accreditation Authority.
559

560 De-authorization of Identity Providers

- 561 t) The authorization policy for Identity providers should include graduated
562 penalties. In other words, not every violation of the policy will result in De-

563 authorization; however, De-authorization may occur if it has been determined
564 that the Identity Provider has materially breached the conditions of its contract
565 and failed to cure based on: a) a third-party complaint received; b) results of an
566 audit or investigation by the Accreditation Auditor or auditor; c) any misuse or
567 abuse of privileges afforded; d) repeated violations of the accreditation policy.
568 Depending upon the nature and circumstances leading to the de-authorization
569 of an Identity Provider, some or all of its outstanding credentials may be
570 revoked or transitioned to a different Identity Provider.

571

572 Accredited entities or individuals:

573 u) MUST agree to:

- 574 ○ only use the data for the legitimate and lawful purpose stated;
- 575 ○ the terms of service, in which the lawful uses of data are described;
- 576 ○ prevent abuse of data received;
- 577 ○ [cooperate with any audit or information requests as a component of an
578 audit;]
- 579 ○ be subject to de-accreditation if they are found to abuse use of data or
580 accreditation policy / requirements;
- 581 ○ store, protect and dispose of the gTLD registration data in accordance
582 with applicable law;
- 583 ○ only retain the gTLD registration data for as long as necessary to achieve
584 the purpose stated in the disclosure request.

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

590

591 Fees:

592 The accreditation service will be a service that is financially sustainable. For further
593 details, see the financial sustainability preliminary recommendation.

594

595 **Implementation Guidance**

596

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

599

- 600 a) Recognized, applicable, and well-established organizations could support the
601 Accreditation Authority as an Identity Provider and/or Verify information.
602 Proper vetting must take place if any such reputable and well-established
603 organizations are to collaborate with the Accreditation Authority.
- 604 b) Examples of additional information the Accreditation Authority or Identity
605 Provider may require an applicant for accreditation to provide could include:

- 606 ○ a business registration number and the name of the authority that
607 issued this number (if the entity applying for accreditation is a legal
608 person);
609 ○ information asserting trademark ownership.
610

611 Auditing / logging by Accreditation Authority and Identity Providers

- 612
- 613 c) The accreditation/verification activity (such as accreditation request,
614 information on the basis of which the decision to accredit or verify identity was
615 made) will be logged by the Accreditation Authority and Identity Providers.
616 d) Logged data shall only be disclosed, or otherwise made available for review, by
617 the Accreditation Authority or Identity Provider, where disclosure is considered
618 necessary to a) fulfill or meet an applicable legal obligation of the Accreditation
619 Authority or Identity Provider; b) carry out an audit under this policy or; c) to
620 support the reasonable functioning of SSAD and the accreditation policy.
621

622 See also auditing and logging preliminary recommendations for further details.
623

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

625

626 **1. Definitions**

- 627 • All definitions of the previous preliminary recommendation apply in
628 addition to:
629 • Eligible government entity: an entity that is considered by its
630 government (including local government) to require access to RDDS data
631 for the exercise of a public policy task.
632

633 **2. Objective of accreditation**

634 SSAD should ensure reasonable access to RDDS for entities that require access to this
635 data for the exercise of their public policy task. In view of their obligations under
636 applicable data protection rules, the final responsibility for granting access to RDDS
637 data will remain with the party that is considered as the controller for the processing of
638 that RDDS data that constitutes personal data.
639

640 Notwithstanding these obligations, the decisions that these data controllers will need
641 to make before granting access to RDDS data to a particular entity, can be greatly
642 facilitated by means of the development and implementation of an accreditation
643 procedure. The accreditation procedure can provide data controllers with information
644 necessary to allow them to assess and decide about the disclosure of data.
645

646 **3. Eligibility**

647 Accreditation by a countries'/territories' government body or its authorized body
648 would be available to various eligible government entities that require access to non-

649 public registration data for the exercise of their public policy task, including, but not
650 limited to:

- 651 • Law enforcement authorities,
- 652 • Judicial authorities,
- 653 • Consumer right's organizations,
- 654 • Cybersecurity authorities, including national Computer Emergency Response
655 Teams (CERTs),
- 656 • Data protection authorities,

657

658 **4. Determining eligibility**

659 Eligible government entities are those that governments consider require access to
660 non-public RDDS data for the exercise of their public policy task, in compliance with
661 applicable data protection laws. Whether an entity should be eligible is determined by
662 a country/territory nominated accreditation authority, without prejudice to the final
663 responsibility of a disclosing party for the processing of personal data following a
664 request for RDDS data.

665

666 **5. Accreditation requirements:**

667 In order to ensure that the accreditation procedure can provide useful information for
668 the data controller to decide whether the RDDS data should be disclosed on the basis
669 of a request from an accredited entity, the accreditation process should take account
670 of a number of requirements.

671

672 The requirements shall be listed and made available to eligible government entities.

673

674 Compliance of accredited entities with these requirements needs to be assured by the
675 accreditation authority. On that basis, accredited parties can be authorized to
676 participate in the SSAD system and receive the necessary access/authentication
677 credentials. In particular, the accreditation authority needs to ensure that an
678 accredited entity respects the following conditions.

679

- 680 • Have a specific and delineated purpose for their access to and use of non-public
681 RDDS data.
- 682 • Represent that access to and use of non-public data is for a lawful purpose and
683 its processing will not be incompatible with the purpose for which it is sought.
- 684 • Have appropriate procedures in place to ensure appropriate identity and access
685 management for individual users in its internal organization.
- 686 • Comply with applicable laws and terms of service to prevent abuse of data
687 accessed.
- 688 • Be subject to, ultimately, de-accreditation if they are found to fall short or in
689 violation of any of these requirements.
- 690 • In cases of violation of any of these requirements, be subject to penalties under
691 applicable laws.

692

693 6. Accreditation procedure

694 Accreditation would be provided by an approved accreditation authority. This authority
695 may be either a countries'/territories' governmental agency (e.g. a Ministry) or
696 delegated to an intergovernmental agency. This authority should publish the
697 requirements for accreditation and carry out the accreditation procedure for eligible
698 government entities.

699

700 • Accreditation emphasizes the responsibilities of the data requestor (recipient),
701 who is responsible for complying with the law.

702 • Accreditation will focus on the requirements of the law, such as requirements
703 regarding data retention length, secure storage, organizational data controls,
704 and breach notifications.

705 • Renewals will incorporate updated terms of service or other obligations
706 imposed by the accreditation authority.

707 • Accredited parties must provide updated accreditation materials with validity
708 dates covering the period of accreditation.

709 • The accreditation authority reserves the right to update what credentials or
710 other material are required for accreditation.

711

712 a. Renewal

713 Accredited/authenticated parties must renew their accreditation/authentication
714 periodically. Each authentication authority should determine an appropriate time limit.

715

716 b. Logging

717 The accreditation authority must log all contact details for the accredited entities and
718 must keep a record of any abuse by the accredited entity. This is without prejudice to
719 any obligation the accreditation authority or the accredited entities may already have
720 to document their use of the system.

721

722 c. Auditing

723 Audits should be conducted by either the data protection authority or by the
724 country/territory designated auditor. This is without prejudice to audits that may
725 carried out by relevant data protection authorities.

726

727 d. Complaints

728 Complaints regarding unauthorized access to, or improper use of, data should be
729 handled by the accreditation authority, for which appropriate procedures should be in
730 place. This is without prejudice to other obligations they may already have under
731 applicable data protection laws to ensure rights of individuals are respected.

732

733 e. Data access

- 734 • Accreditation is required for a party to participate in the access system (SSAD).
735 Unaccredited parties can make data requests outside the system, and
736 contracted parties should have procedures in place to provide reasonable
737 access.
- 738 • Accreditation does not guarantee disclosure of the data. The final responsibility
739 for the decision to disclose data lies with the data controller.
- 740 • Any accredited user will be expected to only process the personal data that it
741 needs to process in order to achieve its processing purposes. They will be
742 obligated to minimize the number of queries they make to those that are
743 reasonably necessary to achieve the purpose.
- 744 • Accredited entities will be required to follow the safeguards as set by the
745 disclosing system.
- 746 • Disclosure of RDDS data to the type of third parties must be made clear to the
747 data subject. Upon a request from a data subject inquiring about the exact
748 processing activities of their data within the SSAD, [relevant information] should
749 be disclosed as soon as reasonably feasible. However the nature of legal
750 investigations or procedures may require SSAD and/or the disclosing entity keep
751 the nature or existence of these requests confidential from the data subject.
752 Confidential requests can be disclosed to data subjects in cooperation with the
753 requesting authority, and in accordance with the data subject's rights under
754 applicable law.
- 755 • Accredited entities should indicate the requirement for confidentiality for any
756 requests where applicable.
- 757 • Accredited entities should provide details to aid the disclosure decision such as
758 any applicable local law relating to the request.
- 759 **f. De-Accreditation**
- 760 • Accredited entities will be subject to graduated penalties, and ultimately de-
761 accreditation if they are found to abuse the system.
- 762 • De-Accreditation will occur when the accreditation authority determines that
763 the Accredited entity has materially breached the conditions of its Accreditation
764 based upon either; a) a third-party complaint received; b) results of an audit or
765 investigation; or c) otherwise for any misuse or abuse of the privileges afforded.
- 766 • De-accreditation will prevent re-accreditation in the future absent special
767 circumstances. De-accreditation procedures will be on reasonable notice to the
768 Accredited party/entity who shall have the right to an appeal.
- 769 • De-accreditation does not prevent the requestor from submitting future
770 requests under the access method provisioned in Recommendation 18 of the
771 EPDP Phase 1 Report, but that they will not be accredited, and thus will be
772 subject to delays, and manual processing.

773

774 Preliminary Recommendation #3. Criteria and Content of Requests

775 The EPDP Team recommends that each SSAD request must include, at a minimum, the
776 following information:

- 777
- 778 a) Domain name pertaining to the request for access/disclosure;
- 779 b) Identification of and information about the requestor (including, requestor's
- 780 accreditation status, if applicable, the nature/type of business entity or individual,
- 781 Power of Attorney statements, where applicable and relevant);
- 782 c) Information about the legal rights of the requestor specific to the request and
- 783 specific rationale and/or justification for the request, (e.g., What is the basis or
- 784 reason for the request; Why is it necessary for the requestor to ask for this data?);
- 785 d) Affirmation that the request is being made in good faith and that data received (if
- 786 any) will be processed lawfully and only in accordance with the justification
- 787 specified in (c);
- 788 e) A list of data elements requested by the requestor, and why the data elements
- 789 requested are adequate, relevant and limited to what is necessary.
- 790

791 The objective of this recommendation is to allow for the standardized submission of

792 requested data elements, including any supporting documentation.

793

794 **Preliminary Recommendation #4. Third Party Purposes/Justifications**

795

796 The EPDP Team recognizes that:

- 797 • Third parties may submit data disclosure requests for specific purposes such as
 - 798 but not limited to: (i) criminal law enforcement, national or public security, (ii)
 - 799 non law enforcement investigations and civil claims, including, intellectual
 - 800 property infringement and UDRP and URS claims, (iii) consumer protection,
 - 801 abuse prevention, digital service provider (DSP) and network security, or (iv)
 - 802 Registered name holder consent or contract.
 - 803 • Assertion of one of these specified purposes does not guarantee access in all
 - 804 cases, but will depend on evaluation of the merits of the specific request,
 - 805 compliance with all applicable policy requirements, and the legal basis for the
 - 806 request.
- 807

808 **Preliminary Recommendation #5. Acknowledgement of receipt**

809

810 The EPDP Team recommends that the response time for acknowledging receipt of a

811 SSAD request by the Central Gateway Manager must be without undue delay, but not

812 more than two (2) hours from receipt.

813

814 The Central Gateway Manager MUST confirm that all required information as per

815 preliminary recommendation #3, criteria and content of request, is provided. Should

816 the Central Gateway Manager determine that the request is incomplete, the Central

817 Gateway Manager must reply to the requestor with an incomplete request response,

818 detailing which required data is missing, and provide an opportunity for the requestor

819 to amend its request.

820

821 The response provided by the Central Gateway Manager should also include
822 information about the subsequent steps as well as the timeline consistent with the
823 recommendations outlined below.

824

825 **Preliminary Recommendation #6. Contracted Party Authorization**

826

- 827 1. The Contracted Party to which the disclosure request has been routed MUST
828 review every request on its merits and MUST NOT disclose data on the basis of
829 accredited user category alone. For the avoidance of doubt, automated review
830 is not explicitly prohibited where it is both legally and technically permissible.
- 831 2. If deemed desirable, the Contracted Party may outsource the authorization
832 responsibility to a third-party provider, but the Contracted Party will remain
833 ultimately responsible for ensuring that the applicable requirements are met.
- 834 3. While the requestor will have the ability to identify the lawful basis under which
835 it expects the Contracted Party to disclose the data requested, the Contracted
836 Party must make the final determination of the appropriate lawful basis for the
837 Contracted Party to disclose the requested information.
- 838 4. The Contracted Party should make a threshold determination (without
839 considering the underlying data) about whether the requestor has established
840 an interest in the disclosure of personal data. The determination should
841 consider the elements:
 - 842 ● Is the identity of the requestor clear/verified?
 - 843 ● Has the requestor provided a legitimate interest or other lawful basis in
844 processing the data?
 - 845 ● Are the data elements requested necessary to the requestor's stated
846 purpose?
 - 847 ○ Necessary means more than desirable but less than
848 indispensable or absolutely necessary.
 - 849 ● The Contracted Party should determine whether the data elements
850 requested are limited and reasonable to achieve the requestor's stated
851 purpose?
 - 852 ○ Each request should be evaluated individually (i.e. each
853 submission should contain a request for data related to a single
854 domain. If a submission relates to multiple domains, each must
855 be evaluated individually.).
 - 856 ○ In addition, each data element in a request should be evaluated
857 individually.

858

859 If the answer to any of the above questions is no, the Contracted Party may
860 deny the request, or require further information from the requestor before
861 proceeding to paragraph 6 below.

862 Absent any legal requirements to the contrary, disclosure cannot be refused
863 solely for lack of any of the following: (i) a court order; (ii) a subpoena; (iii) a
864 pending civil action; or (iv) a UDRP or URS proceeding; nor can refusal to

- 865 disclose be solely based on the fact that the request is founded on alleged
866 intellectual property infringement in content on a website associated with the
867 domain name.
- 868 5. The Contracted Party may evaluate the underlying data requested once the
869 validity of the request is determined under paragraph 4 above. The purpose of
870 paragraph 5 is to determine whether the paragraph 6 meaningful human review
871 is required. The Contracted Party's review of the underlying data should assess
872 at least:
- 873 • Does the data requested contain personal data?
 - 874 ○ If no personal data, no further balancing is required, and the
875 non-personal data MUST be disclosed.
 - 876 • The applicable lawful basis and whether the requested data contains
877 personal data the authorization provider to determine if the balancing
878 test, similar to the requirements under GDPR's 6.1.f, as described in
879 paragraph 6 below is applicable and proceed accordingly.
 - 880 • The Contracted Party should evaluate at least the following factors to
881 determine whether the legitimate interest of the requestor is not
882 outweighed by the interests or fundamental rights and freedoms of the
883 data subject. No single factor is determinative; instead the authorization
884 provider should consider the totality of the circumstances outlined
885 below:
 - 886 • **Assessment of impact.** Consider the direct impact on data subjects as
887 well as any broader possible consequences of the data processing.
888 Whenever the circumstances of the disclosure request or the nature of
889 the data to be disclosed suggest an increased risk for the data subject
890 affected, this shall be taken into account during the decision-making.
 - 891 • **Nature of the data.** Consider the level of sensitivity of the data as well as
892 whether the data is already publicly available.
 - 893 • **Status of the data subject.** Consider whether the data subject's status
894 increases their vulnerability (e.g., children, other protected classes)
 - 895 • **Scope of processing.** Consider information from the disclosure request
896 or other relevant circumstances that indicates whether data will be
897 [securely] held (lower risk) versus publicly disclosed, made accessible to
898 a large number of persons, or combined with other data (higher risk),
899 .[provided that this is not intended to prohibit public disclosures for
900 legal actions or administrative dispute resolution proceedings such as
901 the UDRP or URS].
 - 902 • **Reasonable expectations of the data subject.** Consider whether the
903 data subject would reasonably expect their data to be
904 processed/disclosed in this manner.
 - 905 • **Status of the controller and data subject.** Consider negotiating power
906 and any imbalances in authority between the controller and the data
907 subject.

- 908 • **Legal frameworks involved.** Consider the jurisdictional legal frameworks
909 of the requestor, Contracted Party/Parties, and the data subject, and
910 how this may affect potential disclosures.

911 If, based on consideration of the above factors, the Contracted Party
912 determines that the requestor's legitimate interest is not outweighed by the
913 interests or fundamental rights and freedoms of the data subject, the data **shall**
914 be disclosed. The rationale for the approval **MUST** be documented.

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

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

925

926 **Implementation Guidance**

927

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

938

939 **Preliminary Recommendation #7. Authorization for automated disclosure requests**

940

941 For disclosure requests for which it has been determined that these can be responded
942 to in an automatic fashion (i.e. no human intervention required) the following
943 requirements will apply:

944

- 945 1. The Central Gateway Manager **MUST** confirm that all required information as
946 per preliminary recommendation #3 'criteria and content of requests' is
947 provided and that the request meets the criteria established in these policy
948 recommendations (and is confirmed during the implementation phase) to
949 qualify as an automated disclosure request.
- 950 2. Should the Central Gateway Manager determine that the request is incomplete,
951 the Central Gateway Manager must reply to the requestor with an incomplete

952 request response, detailing which required data is missing, and provide an
953 opportunity for the requestor to amend its request.

954 3. Responses to SSAD requests MUST be provided consistent with the SLAs
955 outlined in preliminary recommendation #8.

956

957 With respect to disclosure requests that would be sent to a Contracted Party for
958 manual evaluation, a Contracted Party MAY request the Central Gateway to fully
959 automate all, or certain types of, disclosure requests, irrespective of the ultimate policy
960 requirements. A Contracted Party MAY retract or revise a request for automation that
961 is not required by these policy recommendations at any time.

962

963 **Implementation Guidance**

964

965 The EPDP Team expects that the following types of disclosure requests can be fully
966 automated (in-take as well as response) from the start:

- 967 • Requests from Law Enforcement in local or otherwise applicable jurisdictions;
- 968 • Responses to UDRP and URS Providers for registrant information verification.

969

970 The EPDP Team will further consider if other types of disclosure requests can be fully
971 automated Day 1. Over time, based on experience gained and/or further legal
972 guidance, the SSAD Advisory Group is expected to provide further guidance on which
973 types of disclosure requests can be fully automated.

974

975 **Preliminary Recommendation #8. Response Requirements**

976

977 For the Central Gateway Manager:

978

979 a) Following receipt of a disclosure request, the Central Gateway Manager MUST
980 confirm¹¹ that all required information as per the preliminary recommendation
981 'criteria and content of requests' is provided (see also preliminary
982 recommendation #5 Acknowledgement of Receipt). Should the Central Gateway
983 Manager establish that the request is incomplete, the Central Gateway
984 Manager MUST provide an opportunity for the requestor to amend and
985 resubmit its request.

986

987 b) Following confirmation that the request is syntactically correct and that all
988 required information has been provided, the Central Gateway Manager MUST
989 immediately and synchronously respond with an acknowledgement response
990 and relay the disclosure request to the responsible Contracted Party, if it does
991 not concern a request that meets the criteria for automatic disclosure.

991

992 c) As part of its relay to the responsible Contracted Party, the Central Gateway
992 Manager MUST provide a recommendation to the Contracted Party whether to

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

993 disclose or not. The Contracted Party MAY follow this recommendation. If the
994 Contracted Party decides not to follow the recommendation of the Central
995 Gateway Manager, the Contracted Party MUST communicate its reasons for not
996 following the Central Gateway Manager recommendation so the Central
997 Gateway Manager can learn and improve on future response
998 recommendations.
999

1000 Contracted Parties:

1001

1002 d) MUST provide a disclosure response without undue delay, unless there are
1003 exceptional circumstances. Such exceptional circumstances may include the
1004 overall number of requests received if the number far exceeds the established
1005 SLAs. SSAD requests that meet the automatic response criteria must receive an
1006 automatic disclosure response. For requests that do not meet the automatic
1007 response criteria, a response must be received in line with the SLAs outlined
1008 below.

1009 e) Responses where disclosure of data (in whole or in part) has been denied
1010 should include: rationale sufficient for the requestor to understand the reasons
1011 for the decision, including, for example, an analysis and explanation of how the
1012 balancing test was applied (if applicable). Additionally, in its response, the entity
1013 receiving the access/disclosure request must include information on how public
1014 registration data can be obtained.
1015

1016 Urgent SSAD Requests

1017 f) A separate accelerated timeline has been recommended for the response to
1018 'Urgent' SSAD Requests, those Requests for which evidence is supplied to show
1019 an immediate need for disclosure (see below). The criteria to determine
1020 whether it concerns an urgent request are limited to circumstances that pose
1021 an imminent threat to life, serious bodily injury, critical infrastructure (online
1022 and offline) or child exploitation. Note that the use of 'Urgent' SSAD Requests is
1023 not limited to LEA.

1024 g) Abuse of urgent requests: Violations of the use of Urgent SSAD Requests will
1025 result in a response from the Central Gateway Manager to ensure that the
1026 requirements for Urgent SSAD Requests are known and met in the first
1027 instance, but repeated violations may result in the Central Gateway Manager
1028 suspending the ability to make urgent requests via the SSAD.

1029 h) Contracted Parties must maintain a dedicated contact for dealing with Urgent
1030 SSAD Requests which can be stored and used by the Central Gateway Manager,
1031 in circumstances where an SSAD request has been flagged as Urgent.
1032 Additionally, the EPDP Team recommends that Contracted Parties MUST
1033 publish their standard business hours and accompanying time zone in the SSAD

1034 portal¹² (or in another standardized place that may be designated by ICANN
1035 from time to time).

1036
1037 The EPDP Team recommends that if the Contracted Party determines that disclosure
1038 would be in violation of applicable laws or result in inconsistency with these policy
1039 recommendations, the Contracted Party must document the rationale and
1040 communicate this information to the requestor and ICANN Compliance (if requested).

1041
1042 If a requestor is of the view that its request was denied erroneously, a complaint
1043 should be filed with ICANN Compliance. ICANN Compliance should be prepared to
1044 investigate complaints regarding disclosure requests under its standard enforcement
1045 processes.

1046
1047 Implementation Guidance:

- 1048
- 1049 a) The Central Gateway Manager MUST confirm that the request is syntactically
1050 correct, including proper and valid Authentication and Signed Assertions.
1051 Should the Central Gateway Manager establish that the request is syntactically
1052 incorrect, the Central Gateway Manager MUST reply with an error response to
1053 the requestor detailing the errors that have been detected.
 - 1054 b) Should the Central Gateway Manager establish that the request is incomplete,
1055 Central Gateway Manager MUST reply with an incomplete request response to
1056 the requestor detailing which data required by policy is missing, providing an
1057 opportunity for the requestor to amend its request.
 - 1058 c) Typically the acknowledgement response will include a “ticket number” or
1059 unique identifier to allow for future interactions with the SSAD.
 - 1060 d) An example of online critical infrastructure¹³ includes, amongst others, root
1061 servers; examples of offline critical infrastructure includes, amongst others,
1062 utilities, transportation and banking.

1063
1064 **Preliminary Recommendation #9. Determining Variable SLAs for response times for**
1065 **SSAD**

1066
1067 **How is priority defined?**

1068
1069 Priority is a code assigned to requests for disclosure that contain agreed to, best effort
1070 target response times.

1071
1072 **Who sets the priority?**

¹² Implementation Guidance: the development of an SSAD Contracted Party profile should be considered that would hold all relevant information, such as standard business hours, jurisdiction, that may be relevant to the requestor would be included.

¹³ For further information, see for example https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

1073
 1074
 1075
 1076
 1077
 1078
 1079
 1080
 1081
 1082
 1083
 1084
 1085
 1086
 1087
 1088
 1089
 1090
 1091
 1092

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 SHALL be communicated to the Central Gateway Manager and Requestor. The Contracted Party shall provide the requested information or provide a reason why it cannot disclose the information under the below-defined response targets and compliance targets.

Priority Matrix for non-automated disclosure requests

Request Type	Priority	Proposed SLA ¹⁴ (for discussion) / Compliance at 6 months / 12 months / 18 months
Urgent Requests “The criteria to determine whether it concerns an urgent request are limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation.”	1	1 business day / 85% / 90% / 95%
Administrative proceedings (such as response to UDRP or URS filing, for example), etc.	2	2 business days / 85% / 90% / 95%
All other requests*	3	See below

1093
 1094
 1095

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

¹⁴ 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.

- 1096 Contracted Party response targets for SSAD requests will occur over two phases:
- 1097 • Phase 1 begins **six (6) months** following the SSAD Policy Effective Date.
 - 1098 • Phase 2 begins **one (1) year** following the SSAD Policy Effective Date.
- 1099 In Phase 1, registrar response targets for SSAD Priority 3 requests will be five (5)
1100 business days. Response targets will be measured using a mean response time, not on
1101 a per-response basis. The SSAD will calculate Contracted Party's mean response target
1102 every 3 months as a rolling average.
- 1103 If Contracted Party fails the five-business day response target, the SSAD will alert
1104 Contracted Party, and Contracted Party will be prompted to provide a rationale to
1105 ICANN as to why the response target is not being met. Failure to provide a rationale to
1106 ICANN within **five (5) business days** will result in an ICANN Compliance inquiry.
- 1107 In Phase 2, Contracted Party compliance targets for SSAD Priority 3 requests will be ten
1108 (10) business days. Similar to the response targets, the compliance target will be
1109 measured using a mean response time, not on a per-response basis. The SSAD will
1110 calculate Contracted Party's mean compliance target every 3 months. If the Contracted
1111 Party's mean compliance target exceeds ten business days, Contracted Party will be
1112 subject to compliance enforcement.
- 1113 Response Targets and Compliance Targets shall be reviewed, at a minimum, annually. A
1114 review mechanism will be further developed by the EPDP Team, but community input
1115 in response to the public comment period will be helpful.
- 1116 The Small Team recommends SSAD response times and associated statistics be as
1117 transparent as legally permissible in order to improve the SSAD and keep the
1118 community informed
- 1119 Response targets for disclosure requests that meet the criteria for fully-automated
1120 responses are expected to be further developed during the implementation phase, but
1121 these are expected to be under 60 seconds.
1122
- 1123 In the event the Mechanism for the continuous evolution of SSAD (see preliminary
1124 recommendation #19 for further details) identifies additional categories of requests
1125 that could be fully automated, the SSAD MUST allow for automation of the processing
1126 of well-formed, valid, complete, properly-identified requests from accredited users
1127 with some limited and specific set of legal basis and data processing purposes which
1128 are yet to be determined. These requests MAY be automatically processed and result in
1129 the disclosure of non-public RDS data without human intervention if legally
1130 permissible.
1131

1132 Preliminary Recommendation #10. Acceptable Use Policy

1133

1134 The EPDP Team recommends that the following requirements are applicable to the
1135 requestor and must be confirmed by the Central Gateway Manager and subject to an
1136 enforcement mechanism. For the avoidance of doubt, every request does not have to
1137 go through an enforcement procedure; the enforcement mechanism may, however, be
1138 triggered in the event of apparent misuse.

1139

1140 The requestor:

1141

- 1142 a) Must only request data from the current RDS data set (no historic data);
- 1143 b) Must, for each request for RDS data, provide representations of the corresponding
1144 purpose and lawful basis for the processing, which will be subject to auditing (see
1145 the auditing preliminary recommendation for further details);
- 1146 c) MAY request data from the SSAD for multiple purposes per request, for the same
1147 set of data requested;
- 1148 d) For each stated purpose must provide (i) representation regarding the intended use
1149 of the requested data and (ii) representation that the requestor will only process
1150 the data for the stated purpose(s). These representations will be subject to auditing
1151 (see auditing preliminary recommendation further details);
- 1152 e) Must handle the data subject's personal data in compliance with applicable law
1153 (see auditing preliminary recommendation for further details).

1154

1155 Preliminary Recommendation #11. Disclosure Requirement

1156

1157 The EPDP Team recommends that the following requirements are applicable to
1158 Contracted Parties and subject to ICANN Compliance enforcement, as well as any
1159 automated responses provided by SSAD. For the avoidance of doubt, every response
1160 does not have to go through an enforcement procedure; the enforcement mechanism
1161 may, however, be triggered in the event of apparent misuse.

1162

1163 Contracted Parties and SSAD:

1164

- 1165 a) Must only disclose the data requested by the requestor;
- 1166 b) Must return current data or a subset thereof in response to a request (no historic
1167 data);
- 1168 c) Must process data in compliance with applicable law;
- 1169 d) Must log requests;
- 1170 e) Where required by applicable law, must perform a balancing test before processing
1171 the data;
- 1172 f) Must disclose to the Registered Name Holder (data subject), on reasonable request,
1173 confirmation of the processing of personal data relating to them, per applicable
1174 law;

- 1175 g) Where required by applicable law, must provide mechanism under which the data
1176 subject may exercise its right to erasure and any other applicable rights;
- 1177 h) Must, in a concise, transparent, intelligible and easily accessible form, using clear
1178 and plain language, provide notice to data subjects of the types of entities/third
1179 parties which may process their data. Notwithstanding obligations on the
1180 Contracted Parties under applicable law, ICANN and the Contracted Parties will
1181 draft and agree upon a privacy policy for the SSAD and standard language (relating
1182 to the SSAD) to inform data subjects according to Art. 13 and 14 GDPR (or any other
1183 relevant obligations), to be presented to data subjects by the Registrars. This will
1184 contain information on potential recipients of non-public registration data
1185 including, but not limited to the recipients listed in Preliminary Recommendation #4
1186 Third Party Purposes / Justifications, as legally permissible. Information duties
1187 according to applicable laws may apply additionally, but the information referenced
1188 above must be contained as a minimum.
- 1189 i) Confidentiality of disclosure requests – Upon a request from a data subject the
1190 exact processing activities of their data within the SSAD, should be disclosed as
1191 soon as reasonably feasible. However the nature of legal investigations or
1192 procedures may require SSAD and/or the disclosing entity keep the nature or
1193 existence of these requests confidential from the data subject. Confidential
1194 requests can be disclosed to data subjects in cooperation with the requesting
1195 authority, [and] [or] in accordance with the data subject’s rights under applicable
1196 law.¹⁵

1197

1198 **Preliminary Recommendation #12. Query Policy**

1199

1200 The EPDP Team recommends that the Central Gateway Manager:

1201

- 1202 a) Must monitor the system and take appropriate action, such as revoking or
1203 limiting access, to protect against abuse or misuse of the system;
- 1204 b) May take measures to limit the number of requests that are submitted by the
1205 same requestor if it is demonstrated that the requests are of an abusive*
1206 nature;

1207

1208 *“Abusive” use of SSAD may include (but is not limited to) the detection of one
1209 or more of the following behaviors/practices:

1210

- 1211 1. High volume automated submissions of malformed or incomplete
1212 requests.
- 1213 2. High volume automated duplicate requests that are frivolous or
1214 vexatious.
- 1215 3. Use of false, stolen or counterfeit credentials to access the system.

¹⁵ The EPDP Team may reconsider this requirement once there is clarity on who will be the entity disclosing the data.

1216 4. Storing/delaying and sending high-volume requests causing the SSAD or
1217 other parties to fail SLA performance. When investigating abuse based
1218 on this specific behavior, the concept of proportionality should be
1219 considered.

1220
1221 As with other access policy violations, abusive behavior can ultimately result in
1222 suspension or termination of access to the SSAD. In the event the entity
1223 receiving requests makes a determination based on abuse to limit the number
1224 of requests a requestor, further to point b, the requestor may seek redress via
1225 ICANN org if it believes the determination is unjustified. For the avoidance of
1226 doubt, if the entity receiving requests receives a high volume of requests from
1227 the same requestor, the volume alone must not result in a de facto
1228 determination of system abuse.

1229
1230 c) MUST respond only to requests for a specific domain name for which non-public
1231 registration data is requested to be disclosed and MUST examine each request
1232 on its own merits.

1233
1234 The EPDP Team recommends the SSAD, in whatever form it eventually takes, MUST:
1235

- 1236 • Support requests keyed on fully qualified domain names (without wildcards).
- 1237 • Support the ability of a requestor to submit multiple domain names in a single
1238 request¹⁶
- 1239 • Route each domain individually to the entity responsible for the disclosure
1240 decision (this may require SSAD to split a request into multiple transactions)
- 1241 • Consider each request on its own merits.
- 1242 • Have the capacity to handle the expected number of requests in alignment with
1243 the SLAs established
- 1244 • Only support requests for current data (no data about the domain name
1245 registration's history).

1246 Requests must only refer to current registration data (historical registration data will
1247 not be made available via this mechanism).

1248
1249 See also the preliminary recommendation #9 (Acceptable Use Policy).

1250
1251 **Preliminary Recommendation #13. Terms of use**

1252
1253 The EPDP Team recommends that appropriate agreements, such as terms of use for
1254 the SSAD, a privacy policy and a disclosure agreement are put in place that take into
1255 account the recommendations from the other preliminary recommendations. These

¹⁶ The EPDP Team expects implementation to reasonably determine how many may be submitted at a time and consistent with the Query Policy.

1256 agreements are expected to be developed and negotiated by the parties involved in
1257 SSAD, taking the below implementation guidance into account.

1258

1259 Implementation guidance:

1260

1261 Privacy Policy for SSAD Users

1262

1263 The EPDP recommends, at a minimum, the privacy policy shall include:

1264

- Relevant data protection principles, for example,

1265

- The type(s) of personal data processed

1266

- How and why the personal data is processed, for example,

1267

- verifying identity

1268

- communicating service notices

1269

- How long personal data will be retained

1270

- The types of third parties with whom personal data is shared

1271

- Where applicable, details of any international data transfers/requirements

1272

thereof

1273

- Information about the data subject rights and the method by which they can

1274

exercise these rights

1275

- Notification of how changes to the privacy policy will be communicated

1276

1277 Further consideration should be given during implementation whether updates to the

1278

RAA are necessary to ensure compliance with these recommendations.

1279

1280 Terms of Use

1281

1282 The EPDP recommends, at a minimum, the terms of use shall address:

1283

- Indemnification of the controllers based on the following principles:

1285

- Requestors are responsible for damages or costs related to third party

1286

claims arising from (i) their misrepresentations in the accreditation or

1287

request process; or (ii) misuse of the requested data in violation of the

1288

applicable terms of use or applicable law(s).

1289

- Nothing in these terms limits any parties' liability or rights of recovery

1290

under applicable laws (i.e. requestors are not precluded from seeking

1291

recovery from controllers where those rights are provided under law).

1292

- Nothing in these terms shall be construed to create indemnification

1293

obligations for public authority requestors who lack the legal authority

1294

to enter into such indemnification clauses. Further, nothing in this clause

1295

shall alter potentially existing government liability as a recourse for the

1296

operators of the SSAD.

1297

- Data request requirements

1298

- Logging requirements

1299

- Ability to demonstrate compliance

- 1300 • Applicable prohibitions

1301

1302 Disclosure agreements

1303

1304 The EPDP recommends, at a minimum, disclosure agreements shall address:

1305

- 1306 • Use of the data for the purpose indicated in the request
- 1307 • Requirements for use of data for a new purpose other than the one indicated in
- 1308 the request
- 1309 • Retention of data
- 1310 • Lawful use of data

1311

1312 **Preliminary Recommendation #14. Retention and Destruction of Data**

1313

1314 The EPDP Team recommends that requestors must confirm that they will store, protect
1315 and dispose of the gTLD registration data in accordance with applicable law.

1316 Requestors must retain only the gTLD registration data for as long as necessary to
1317 achieve the purpose stated in the disclosure request.

1318

1319 **Preliminary Recommendation #15. Financial Sustainability**

1320

1321 The EPDP Team recommends that, in considering the costs and financial sustainability
1322 of SSAD, one needs to distinguish between the development and operationalization of
1323 the system and the subsequent running of the system.

1324

1325 The EPDP Team expects that the costs for developing, deployment and operationalizing
1326 the system, similar to the implementation of other adopted policy recommendations,
1327 to be initially borne by ICANN org, Contracted Parties and other parties that may be
1328 involved. It is the EPDP Team's expectation that the SSAD will ultimately result in equal
1329 or lesser costs to Contracted Parties compared to manual receipt and review of
1330 requests.

1331

1332 The subsequent running of the system is expected to happen on a cost recovery basis
1333 whereby historic costs may be considered. For example, if the SSAD includes an
1334 accreditation framework under which users of the SSAD could become accredited, the
1335 costs associated with becoming accredited would be borne by those seeking
1336 accreditation. Similarly, some of the cost of running the SSAD may be offset by charging
1337 fees to the users of the SSAD.

1338

1339 When implementing and operating the SSAD, a disproportionately high burden on
1340 smaller operators should be avoided.

1341

1342 The EPDP Team recognizes that the fees associated with using the SSAD may differ for
1343 users based on request volume or user type (e.g. governments may have restrictions

1344 from paying) among other potential factors. The EPDP Team also recognizes that
1345 governments may be subject to certain payment restrictions.

1346
1347 The objective is that the SSAD is financially self-sufficient without causing any
1348 additional fees for registrants. Data subjects MUST NOT bear the costs for having their
1349 data disclosed to third parties; requestors of the SSAD data should primarily bear the
1350 costs of maintaining this system. ICANN may contribute to the (partial) covering of
1351 costs for maintaining the Central Gateway.

1352
1353 The SSAD should not be considered a profit-generating platform for ICANN or the
1354 contracted parties. Funding for the SSAD should be sufficient to cover costs, including
1355 for subcontractors at market cost and to establish a legal risk fund. It is crucial to
1356 ensure that any payments in the SSAD are related to operational costs and are not
1357 simply an exchange of money for non-public registration data.

1358
1359 In relation to the accreditation framework:
1360 a) Accreditation applicants may be charged a to-be-determined non-refundable
1361 fee proportional to the cost of validating an application.
1362 b) Rejected applicants may re-apply, but the new application(s) may be subject to
1363 the application fee.
1364 c) Fees are to be established by the accreditation authority.
1365 d) Accredited users and organizations must renew their accreditation periodically.

1366
1367 **Implementation guidance:** (associated with disclosure requests):
1368 Given the number of policy options implicit in the various models, there are various
1369 implementation details that may have policy implications, particularly with respect to
1370 cost distribution and choice of party who performs various data protection functions.
1371 These issues are collected here under Implementation Guidance for consideration.

1372
1373 The fee structure as well as the renewal period is to be determined in the
1374 implementation phase, following the principles outlined above. The EPDP Team
1375 recognizes that it may not be possible to set the exact fees until the actual costs are
1376 known. The EPDP Team also recognizes that the SSAD fee structure may need to be
1377 reviewed over time.

1378
1379 Placeholders

1380
1381 The EPDP Team will further consider whether the resubmission of a request will be
1382 treated as a new request from a cost/fee perspective.

1383
1384 The EPDP Team has requested input from ICANN Org concerning the expected costs of
1385 developing, operationalizing and maintaining the three different models. Based on the
1386 feedback received, the EPDP Team may develop further guidance in relation to the
1387 financial sustainability of SSAD.

1388

1389 Preliminary Recommendation #16. Automation

1390

1391 The EPDP Team acknowledges that full automation of the SSAD may not be possible,
1392 but recommends that the SSAD must be automated where technically feasible, legally
1393 permissible and financially (or commercially) reasonable.¹⁷ Additionally, in areas where
1394 automation is not both technically feasible and legally permissible, the EPDP Team
1395 recommends standardization as the baseline objective.

1396

1397 For example, the EPDP Team expects that aspects of the SSAD such as intake of
1398 requests, credential check, request submission validation (format & completeness, not
1399 content) could be automated, while it may not be possible to completely automate all
1400 request review and disclosure.

1401

1402 The SSAD must allow for the automation of syntax checking of incoming requests,
1403 resulting in an automatic response that indicates the errors to the requestor. This
1404 automation addresses the risk of filling up the request queues of the discloser with
1405 malformed requests.

1406

1407 The SSAD must allow for the automation of checking that the contents of a request is
1408 complete, per policy, resulting in an automatic response that provides details
1409 explaining what elements are incomplete. This automation allows for the discloser to
1410 indicate - without human intervention - if any additional information is required per
1411 policy and enables the requestor to address the error.

1412

1413 The SSAD must allow for the automation of an immediate and synchronous response
1414 that indicates the receipt of a valid request and some indication that it will be
1415 processed. Typically, such responses include a "ticket number" or some kind of unique
1416 ID to allow for future queries (status, updates, deletion, etc.). This automation allows
1417 for efficient queue management on the discloser's side and assists in ensuring the
1418 principal of "predictability" is met.

1419

1420 The SSAD must allow for automation of the processing of well-formed, valid, complete,
1421 properly-identified requests from accredited users with some limited and specific set of
1422 legal basis and data processing purposes which are yet to be determined. These
1423 requests MAY be automatically processed and result in the disclosure of non-public
1424 RDS data without human intervention.

1425

1426 Preliminary Recommendation #17. Logging

1427

¹⁷ Initial consideration of the financial feasibility of automation will be addressed by the Implementation Review Team and subsequently by the mechanism for the continuous evolution of SSAD, as applicable.

1428 The EPDP Team expects that the appropriate logging procedures are put in place to
1429 facilitate the auditing procedures outlined in these recommendations. These logging
1430 requirements will cover the following:

1431

- 1432 ● Accreditation authority
- 1433 ● Central Gateway Manager
- 1434 ● Identity provider
- 1435 ● Activity of accredited users such as login attempts, queries
- 1436 ● What queries and disclosure decision(s) are made¹⁸

1437

1438 The EPDP Team recommends:

1439

1440 a) The activity of all SSAD entities will be logged. (for further details, please see the
1441 implementation guidance below).

1442 b) Logs will include a record of all queries and all items necessary to audit any
1443 decisions made in the context of SSAD.

1444 c) Logs must be retained for a period sufficient for auditing and complaint
1445 resolution purposes, taking into account statutory limits related to complaints
1446 against the controller.

1447 d) Logs must be retained in a commonly used, structured, machine-readable
1448 format accompanied by an intelligible description of all variables.

1449 e) Logged data will remain confidential and must be disclosed in the following
1450 circumstances:

1451 i. In the event of a claim of misuse, logs may be requested for examination
1452 by an accreditation authority or dispute resolution provider.

1453 ii. Logs should be further available to data protection authorities, ICANN,
1454 and the auditing body.¹⁹

1455 iii. When mandated as a result of due legal process, including relevant
1456 supervisory authorities, as applicable.

1457 iv. General technical operation to ensure proper running of the system.

1458

1459 Implementation guidance:

1460

1461 At a minimum, the following events must be logged

- 1462 ● Logging related to the Identity Provider
- 1463 ● Logging related to the accreditation provider
 - 1464 ○ Details of incoming requests for Accreditation

¹⁸ Note, EPDP Team to review at a later stage as the ability for SSAD to log this information depends on who is the entity that makes the disclosure decision

¹⁹ Note, EPDP Team to review at a later stage as there is a question of the set-up of the system of whether or not the Ry and RR as Controllers (where liability remains with them) may require access to the logs for them to engage in audit, or answer Data Subject requests.

- 1465 ○ Results of processing requests for Accreditation, e.g., issuance of the
- 1466 Identity Credential or reasons for denial
- 1467 ○ Details of Revocation Requests
- 1468 ○ Indication when Identity Credentials and Signed Assertions have been
- 1469 Validated.
- 1470 ○ Unique reference number
- 1471 ● Logging related to the Central Gateway Manager
- 1472 ○ Information related to the contents of the query itself.
- 1473 ○ Results of processing the query, including changes of state (e.g.,
- 1474 received, pending, in-process, denied, approved, approved with
- 1475 changes)
- 1476 ● Logging related to the entity Authorizing the request
- 1477 ○ Request Response details, e.g., Reason for denial, Notice of approval and
- 1478 data elements released. Disclosure decisions including a written
- 1479 rationale must be stored and put in escrow so it can be accessed by
- 1480 ICANN and the contracted parties in case of objections or legal claims
- 1481 raised to support a legal defense.
- 1482

1483 **Preliminary Recommendation #18. Audits**

1484

1485 The EPDP Team expects that the appropriate auditing processes and procedures are
1486 put in place to ensure appropriate monitoring and compliance with the requirements
1487 outlined in these recommendations.

1488

1489 As part of any audit, the auditor MUST be subject to reasonable confidentiality
1490 obligations with respect to proprietary processes and personal information disclosed
1491 during the audit.

1492

1493 More specifically:

1494

1495 **Audits of the Accrediting Authority**

1496

1497 If ICANN outsources the accreditation authority function to a qualified third party, the
1498 accrediting authority MUST be audited periodically to ensure compliance with the
1499 policy requirements as defined in the accreditation preliminary recommendation.

1500 Should the accreditation authority be found in breach of the accreditation policy and
1501 requirements, it will be given an opportunity to cure the breach, but in cases of
1502 repeated non-compliance or audit failure, a new accreditation authority must be
1503 identified or created.

1504

1505 Any audit of the accreditation authority shall be tailored for the purpose of assessing
1506 compliance, and the auditor MUST give reasonable advance notice of any such audit,
1507 which notice shall specify in reasonable detail the categories of documents, data, and
1508 other information requested.

1509

1510 As part of such audits, the accreditation authority shall provide to the auditor in a
1511 timely manner all responsive documents, data, and any other information necessary to
1512 demonstrate its compliance with the accreditation policy.

1513

1514 If ICANN serves as the accreditation authority, existing accountability mechanisms are
1515 expected to address any [policy] breaches, noting that in such an extreme case,
1516 requirements for other entities involved in SSAD may be temporarily lifted until a
1517 confirmed breach has been addressed.

1518

1519 As ICANN serves as the accreditation authority, existing accountability mechanisms are
1520 expected to address any breaches of the accreditation policy, noting that in such an
1521 extreme case, the credentials issued during the time of the breach will be reviewed.
1522 Modalities of this review should be established in the implementation phase.

1523

1524 **Audits of Identity Provider(s)**

1525

1526 Identity Providers **MUST** be audited periodically to ensure compliance with the policy
1527 requirements as defined in the accreditation preliminary recommendation. Should the
1528 Identity Provider be found in breach of the accreditation policy and requirements, it
1529 will be given an opportunity to cure the breach, but in cases of repeated non-
1530 compliance or audit failure, a new Identity Provider must be identified.

1531

1532 Any audit of an Identity Provider shall be tailored for the purpose of assessing
1533 compliance, and the auditor **MUST** give reasonable advance notice of any such audit,
1534 which notice shall specify in reasonable detail the categories of documents, data and
1535 other information requested.

1536

1537 As part of such audits, the Identity Provider shall provide to the auditor in a timely
1538 manner all responsive documents, data, and any other information necessary to
1539 demonstrate its compliance with the accreditation policy.

1540

1541 **Audits of Accredited Entities/Individuals**

1542

1543 Appropriate mechanisms must be developed in the implementation phase to ensure
1544 accredited entities' and individuals' compliance with the policy requirements as
1545 defined in the accreditation preliminary recommendation. These could include, for
1546 example, audits triggered by complaints, random audits, or audits in response to a self-
1547 certification or self-assessment. Should the accredited entity or individual be found in
1548 breach of the accreditation policy and requirements, it will be given an opportunity to
1549 cure the breach, but in cases of repeated non-compliance or audit failure the matter
1550 should be referred back to the Accreditation Authority and/or Identity Provider, if
1551 applicable, for action.

1552

1553 Any audit of accredited entities/individuals shall be tailored for the purpose of
1554 assessing compliance, and the auditor MUST give reasonable advance notice of any
1555 such audit, which notice shall specify in reasonable detail the categories of documents,
1556 data and other information requested.

1557

1558 As part of such audits, the accredited entity/individual shall, in a timely manner,
1559 provide to the auditor all responsive documents, data, and any other information
1560 necessary to demonstrate its compliance with the accreditation policy.

1561

1562 **Audits of the Central Gateway Manager & Contracted Parties**

1563

1564 The EPDP Team will further consider these requirements once the EPDP Team has
1565 decided on the roles and responsibilities of the different parties in the SSAD.

1566

1567 **Preliminary Recommendation #19. Mechanism for the continuous evolution of SSAD**

1568

1569 In conjunction with the implementation of these recommendations, the EPDP
1570 recommends the creation of a Mechanism for the continuous evolution of SSAD. This
1571 Mechanism has the responsibility to provide guidance on the following topics:

1572

- 1573 a) SLA matrix review;
- 1574 b) Categories of disclosure requests which should be automated;
- 1575 c) Other implementation improvements such as the identification of possible user
1576 categories and/or disclosure rationales.

1577

1578 The Mechanism focuses solely on the implementation of the SSAD and must not
1579 contravene the ICANN Bylaws, the GNSO PDP and/or existing contractual provisions for
1580 the development of new requirements for Contracted Parties. The Mechanism may
1581 make recommendations to the GNSO Council for any policy issues that may require
1582 further policy work.

1583

1584 The EPDP Team has indicated a preference to use existing processes and procedures to
1585 establish this Mechanism, if possible. Similarly, unnecessary complexity or cost should
1586 be avoided. The EPDP Team will further consider the details of the Mechanism, and
1587 would like request community input on the following:

1588

1589

1590

1591

1592

1593

1594

1595

1596

- What existing processes / procedures, if any, can be used to meet the above responsibilities?
- If no suitable existing processes / procedures can be used, what type of mechanism should be created factoring in:
 - Who should guidance be provided to?
 - How is guidance developed / agreed to?
 - How should it be structured?
- What information is needed to ensure the continuous evolution of SSAD?
- How is guidance of the Mechanism expected to be implemented?

1597

1598 A detailed charter for the Mechanism is expected to be developed during the
1599 implementation phase of these policy recommendations.

1600

1601 **SSAD Implementation Guidance**

1602

1603 **Implementation Guidance #i.**

1604 The EPDP Team recommends that, consistent with the preliminary recommendation
1605 that an SSAD request must be received for each domain name registration for which
1606 non-public registration is requested to be disclosed, it must be possible for requestors
1607 to submit multiple requests at the same time, for example, by entering multiple
1608 domain name registrations in the same request form if the same request information
1609 applies.

1610

1611

1612

1613

1614

1615

4 Next Steps

1616

4.1 Next Steps

1617

1618

The EPDP Team will complete the next phase of its work and develop its

1619

recommendations in a Final Report to be sent to the GNSO Council for review following

1620

its analysis of public comments received on this Initial Report. If adopted by the GNSO

1621

Council, the Final Report would then be forwarded to the ICANN Board of Directors for

1622

its consideration and, potentially, approval as an ICANN Consensus Policy.

1623

1624

1625

Glossary

1626

1627

1. Advisory Committee

1628

An Advisory Committee is a formal advisory body made up of representatives from the

1629

Internet community to advise ICANN on a particular issue or policy area. Several are

1630

mandated by the ICANN Bylaws and others may be created as needed. Advisory

1631

committees have no legal authority to act for ICANN, but report their findings and

1632

make recommendations to the ICANN Board.

1633

2. ALAC - At-Large Advisory Committee

1634

ICANN's At-Large Advisory Committee (ALAC) is responsible for considering and

1635

providing advice on the activities of the ICANN, as they relate to the interests of

1636

individual Internet users (the "At-Large" community). ICANN, as a private sector, non-

1637

profit corporation with technical management responsibilities for the Internet's

1638

domain name and address system, will rely on the ALAC and its supporting

1639

infrastructure to involve and represent in ICANN a broad set of individual user

1640

interests.

1641

3. Business Constituency

1642

The Business Constituency represents commercial users of the Internet. The Business

1643

Constituency is one of the Constituencies within the Commercial Stakeholder Group

1644

(CSG) referred to in Article 11.5 of the ICANN bylaws. The BC is one of the stakeholder

1645

groups and constituencies of the Generic Names Supporting Organization (GNSO)

1646

charged with the responsibility of advising the ICANN Board on policy issues relating to

1647

the management of the domain name system.

1648

1649

4. ccNSO - The Country-Code Names Supporting Organization

1650

The ccNSO the Supporting Organization responsible for developing and recommending

1651

to ICANN's Board global policies relating to country code top-level domains. It provides

1652

a forum for country code top-level domain managers to meet and discuss issues of

1653

concern from a global perspective. The ccNSO selects one person to serve on the

1654

board.

1655

5. ccTLD - Country Code Top Level Domain

1656

ccTLDs are two-letter domains, such as .UK (United Kingdom), .DE (Germany) and .JP

1657

(Japan) (for example), are called country code top level domains (ccTLDs) and

1658

correspond to a country, territory, or other geographic location. The rules and policies

1659

for registering domain names in the ccTLDs vary significantly and ccTLD registries limit

1660

use of the ccTLD to citizens of the corresponding country.

1661

For more information regarding ccTLDs, including a complete database of designated

1662

ccTLDs and managers, please refer to <http://www.iana.org/cctld/cctld.htm>.

1663 **6. Domain Name Registration Data**

1664 Domain name registration data, also referred to registration data, refers to the
1665 information that registrants provide when registering a domain name and that
1666 registrars or registries collect. Some of this information is made available to the public.
1667 For interactions between ICANN Accredited Generic Top-Level Domain (gTLD) registrars
1668 and registrants, the data elements are specified in the current RAA. For country code
1669 Top Level Domains (ccTLDs), the operators of these TLDs set their own or follow their
1670 government's policy regarding the request and display of registration information.

1671 **7. Domain Name**

1672 As part of the Domain Name System, domain names identify Internet Protocol
1673 resources, such as an Internet website.

1674

1675 **8. DNS - Domain Name System**

1676 DNS refers to the Internet domain-name system. The Domain Name System (DNS)
1677 helps users to find their way around the Internet. Every computer on the Internet has a
1678 unique address - just like a telephone number - which is a rather complicated string of
1679 numbers. It is called its "IP address" (IP stands for "Internet Protocol"). IP Addresses are
1680 hard to remember. The DNS makes using the Internet easier by allowing a familiar
1681 string of letters (the "domain name") to be used instead of the arcane IP address. So
1682 instead of typing 207.151.159.3, you can type www.internic.net. It is a "mnemonic"
1683 device that makes addresses easier to remember.

1684

1685 **9. EPDP – Expedited Policy Development Process**

1686 A set of formal steps, as defined in the ICANN bylaws, to guide the initiation, internal
1687 and external review, timing and approval of policies needed to coordinate the global
1688 Internet's system of unique identifiers. An EPDP may be initiated by the GNSO Council
1689 only in the following specific circumstances: (1) to address a narrowly defined policy
1690 issue that was identified and scoped after either the adoption of a GNSO policy
1691 recommendation by the ICANN Board or the implementation of such an adopted
1692 recommendation; or (2) to provide new or additional policy recommendations on a
1693 specific policy issue that had been substantially scoped previously, such that extensive,
1694 pertinent background information already exists, e.g. (a) in an Issue Report for a
1695 possible PDP that was not initiated; (b) as part of a previous PDP that was not
1696 completed; or (c) through other projects such as a GNSO Guidance Process.

1697 **10. GAC - Governmental Advisory Committee**

1698 The GAC is an advisory committee comprising appointed representatives of national
1699 governments, multi-national governmental organizations and treaty organizations, and
1700 distinct economies. Its function is to advise the ICANN Board on matters of concern to
1701 governments. The GAC will operate as a forum for the discussion of government
1702 interests and concerns, including consumer interests. As an advisory committee, the
1703 GAC has no legal authority to act for ICANN, but will report its findings and
1704 recommendations to the ICANN Board.

1705 **11. General Data Protection Regulation (GDPR)**

1706 The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law
1707 on data protection and privacy for all individuals within the European Union (EU) and
1708 the European Economic Area (EEA). It also addresses the export of personal data
1709 outside the EU and EEA areas.

1710

1711 **12. GNSO - Generic Names Supporting Organization**

1712 The supporting organization responsible for developing and recommending to the
1713 ICANN Board substantive policies relating to generic top-level domains. Its members
1714 include representatives from gTLD registries, gTLD registrars, intellectual property
1715 interests, Internet service providers, businesses and non-commercial interests.

1716 **13. Generic Top Level Domain (gTLD)**

1717 "gTLD" or "gTLDs" refers to the top-level domain(s) of the DNS delegated by ICANN
1718 pursuant to a registry agreement that is in full force and effect, other than any country
1719 code TLD (ccTLD) or internationalized domain name (IDN) country code TLD.

1720 **14. gTLD Registries Stakeholder Group (RySG)**

1721 The gTLD Registries Stakeholder Group (RySG) is a recognized entity within the Generic
1722 Names Supporting Organization (GNSO) formed according to Article X, Section 5
1723 (September 2009) of the Internet Corporation for Assigned Names and Numbers
1724 (ICANN) Bylaws.

1725

1726 The primary role of the RySG is to represent the interests of gTLD registry operators (or
1727 sponsors in the case of sponsored gTLDs) ("Registries") (i) that are currently under
1728 contract with ICANN to provide gTLD registry services in support of one or more gTLDs;
1729 (ii) who agree to be bound by consensus policies in that contract; and (iii) who
1730 voluntarily choose to be members of the RySG. The RySG may include Interest Groups
1731 as defined by Article IV. The RySG represents the views of the RySG to the GNSO
1732 Council and the ICANN Board of Directors with particular emphasis on ICANN
1733 consensus policies that relate to interoperability, technical reliability and stable
1734 operation of the Internet or domain name system.

1735

1736 **15. ICANN - The Internet Corporation for Assigned Names and Numbers**

1737 The Internet Corporation for Assigned Names and Numbers (ICANN) is an
1738 internationally organized, non-profit corporation that has responsibility for Internet
1739 Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD)
1740 and country code (ccTLD) Top-Level Domain name system management, and root
1741 server system management functions. Originally, the Internet Assigned Numbers
1742 Authority (IANA) and other entities performed these services under U.S. Government
1743 contract. ICANN now performs the IANA function. As a private-public partnership,
1744 ICANN is dedicated to preserving the operational stability of the Internet; to promoting
1745 competition; to achieving broad representation of global Internet communities; and to

1746 developing policy appropriate to its mission through bottom-up, consensus-based
1747 processes.

1748 **16. Intellectual Property Constituency (IPC)**

1749 The Intellectual Property Constituency (IPC) represents the views and interests of the
1750 intellectual property community worldwide at ICANN, with a particular emphasis on
1751 trademark, copyright, and related intellectual property rights and their effect and
1752 interaction with Domain Name Systems (DNS). The IPC is one of the constituency
1753 groups of the Generic Names Supporting Organization (GNSO) charged with the
1754 responsibility of advising the ICANN Board on policy issues relating to the management
1755 of the domain name system.

1756

1757 **17. Internet Service Provider and Connectivity Provider Constituency (ISPCP)**

1758 The ISPs and Connectivity Providers Constituency is a constituency within the GNSO.
1759 The Constituency's goal is to fulfill roles and responsibilities that are created by
1760 relevant ICANN and GNSO bylaws, rules or policies as ICANN proceeds to conclude its
1761 organization activities. The ISPCP ensures that the views of Internet Service Providers
1762 and Connectivity Providers contribute toward fulfilling the aims and goals of ICANN.

1763

1764 **18. Name Server**

1765 A Name Server is a DNS component that stores information about one zone (or more)
1766 of the DNS name space.

1767 **19. Non Commercial Stakeholder Group (NCSG)**

1768 The Non Commercial Stakeholder Group (NCSG) is a Stakeholder Group within the
1769 GNSO. The purpose of the Non Commercial Stakeholder Group (NCSG) is to represent,
1770 through its elected representatives and its Constituencies, the interests and concerns
1771 of noncommercial registrants and noncommercial Internet users of generic Top-level
1772 Domains (gTLDs). It provides a voice and representation in ICANN processes to: non-
1773 profit organizations that serve noncommercial interests; nonprofit services such as
1774 education, philanthropies, consumer protection, community organizing, promotion of
1775 the arts, public interest policy advocacy, children's welfare, religion, scientific research,
1776 and human rights; public interest software concerns; families or individuals who
1777 register domain names for noncommercial personal use; and Internet users who are
1778 primarily concerned with the noncommercial, public interest aspects of domain name
1779 policy.

1780

1781 **20. Post Delegation Dispute Resolution Procedures (PDDRPs)**

1782 Post-Delegation Dispute Resolution Procedures have been developed to provide those
1783 harmed by a new gTLD Registry Operator's conduct an alternative avenue to complain
1784 about that conduct. All such dispute resolution procedures are handled by providers
1785 external to ICANN and require that complainants take specific steps to address their
1786 issues before filing a formal complaint. An Expert Panel will determine whether a
1787 Registry Operator is at fault and recommend remedies to ICANN.

1788

1789 21. Registered Name

1790 "Registered Name" refers to a domain name within the domain of a gTLD, whether
1791 consisting of two (2) or more (e.g., john.smith.name) levels, about which a gTLD
1792 Registry Operator (or an Affiliate or subcontractor thereof engaged in providing
1793 Registry Services) maintains data in a Registry Database, arranges for such
1794 maintenance, or derives revenue from such maintenance. A name in a Registry
1795 Database may be a Registered Name even though it does not appear in a zone file (e.g.,
1796 a registered but inactive name).

1797

1798 22. Registrar

1799 The word "registrar," when appearing without an initial capital letter, refers to a person
1800 or entity that contracts with Registered Name Holders and with a Registry Operator
1801 and collects registration data about the Registered Name Holders and submits
1802 registration information for entry in the Registry Database.

1803

1804 23. Registrars Stakeholder Group (RrSG)

1805 The Registrars Stakeholder Group is one of several Stakeholder Groups within the
1806 ICANN community and is the representative body of registrars. It is a diverse and active
1807 group that works to ensure the interests of registrars and their customers are
1808 effectively advanced. We invite you to learn more about accredited domain name
1809 registrars and the important roles they fill in the domain name system.

1810

1811 24. Registry Operator

1812 A "Registry Operator" is the person or entity then responsible, in accordance with an
1813 agreement between ICANN (or its assignee) and that person or entity (those persons or
1814 entities) or, if that agreement is terminated or expires, in accordance with an
1815 agreement between the US Government and that person or entity (those persons or
1816 entities), for providing Registry Services for a specific gTLD.

1817 25. Registration Data Directory Service (RDDS)

1818 Domain Name Registration Data Directory Service or RDDS refers to the service(s)
1819 offered by registries and registrars to provide access to Domain Name Registration
1820 Data.

1821

1822 26. Registration Restrictions Dispute Resolution Procedure (RRDRP)

1823 The Registration Restrictions Dispute Resolution Procedure (RRDRP) is intended to
1824 address circumstances in which a community-based New gTLD Registry Operator
1825 deviates from the registration restrictions outlined in its Registry Agreement.

1826

1827 27. SO - Supporting Organizations

1828 The SOs are the three specialized advisory bodies that advise the ICANN Board of
1829 Directors on issues relating to domain names (GNSO and CCNSO) and, IP addresses
1830 (ASO).

1831 **28. SSAC - Security and Stability Advisory Committee**

1832 An advisory committee to the ICANN Board comprised of technical experts from
1833 industry and academia as well as operators of Internet root servers, registrars and TLD
1834 registries.

1835 **29. TLD - Top-level Domain**

1836 TLDs are the names at the top of the DNS naming hierarchy. They appear in domain
1837 names as the string of letters following the last (rightmost) ".", such as "net" in
1838 <http://www.example.net>. The administrator for a TLD controls what second-level
1839 names are recognized in that TLD. The administrators of the "root domain" or "root
1840 zone" control what TLDs are recognized by the DNS. Commonly used TLDs include
1841 .COM, .NET, .EDU, .JP, .DE, etc.

1842 **30. Uniform Dispute Resolution Policy (UDRP)**

1843 The Uniform Dispute Resolution Policy (UDRP) is a rights protection mechanism that
1844 specifies the procedures and rules that are applied by registrars in connection with
1845 disputes that arise over the registration and use of gTLD domain names. The UDRP
1846 provides a mandatory administrative procedure primarily to resolve claims of abusive,
1847 bad faith domain name registration. It applies only to disputes between registrants and
1848 third parties, not disputes between a registrar and its customer.

1849 **31. Uniform Rapid Suspension (URS)**

1850 The Uniform Rapid Suspension System is a rights protection mechanism that
1851 complements the existing Uniform Domain-Name Dispute Resolution Policy (UDRP) by
1852 offering a lower-cost, faster path to relief for rights holders experiencing the most
1853 clear-cut cases of infringement.
1854

1855

1856 **32. WHOIS**

1857 WHOIS protocol is an Internet protocol that is used to query databases to obtain
1858 information about the registration of a domain name (or IP address). The WHOIS
1859 protocol was originally specified in RFC 954, published in 1985. The current
1860 specification is documented in RFC 3912. ICANN's gTLD agreements require registries
1861 and registrars to offer an interactive web page and a port 43 WHOIS service providing
1862 free public access to data on registered names. Such data is commonly referred to as
1863 "WHOIS data," and includes elements such as the domain registration creation and
1864 expiration dates, nameservers, and contact information for the registrant and
1865 designated administrative and technical contacts.

1866

1867 WHOIS services are typically used to identify domain holders for business purposes and
1868 to identify parties who are able to correct technical problems associated with the
1869 registered domain.

1870

1871
1872
1873
1874

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

ISSUE DESCRIPTION AND/OR CHARTER QUESTIONS

1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908

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?

- 1909 c5) What kinds of insights will Contracted Parties have into what data is
1910 accessed and how it is used?
1911 c6) What rights do data subjects have in ascertaining when and how their data
1912 is accessed and used?
1913 c7) How can a third party access model accommodate differing requirements
1914 for data subject notification of data disclosure?
1915

1916 From the Annex to the Temporary Specification:
1917

- 1918 ● Developing methods to provide potential URS and UDRP complainants with
1919 sufficient access to Registration Data to support good-faith filings of complaints
- 1920 ● Limitations in terms of query volume envisaged under an accreditation program
1921 balanced against realistic investigatory cross-referencing needs.
- 1922 ● Confidentiality of queries for Registration Data by law enforcement authorities
- 1923 ● Pursuant to Section 4.4, continuing community work to develop an
1924 accreditation and access model that complies with GDPR, while recognizing the
1925 need to obtain additional guidance from Article 29 Working Party/European
1926 Data Protection Board.
- 1927 ● Consistent process for continued access to Registration Data, including non-
1928 public data, for users with a legitimate purpose, until the time when a final
1929 accreditation and access mechanism is fully operational, on a mandatory basis
1930 for all contracted parties.

1931

1932 From EPDP Team Phase 1 Final Report:
1933

1934 EPDP Team Recommendation #3.

1935 In accordance with the EPDP Team Charter and in line with Purpose #2, the EPDP Team
1936 undertakes to make a recommendation pertaining to a standardised model for lawful
1937 disclosure of non-public Registration Data (referred to in the Charter as 'Standardised
1938 Access') now that the gating questions in the charter have been answered. This will
1939 include addressing questions such as:

1940

- 1941 ● Whether such a system should be adopted
- 1942 ● What are the legitimate purposes for third parties to access registration data?
- 1943 ● What are the eligibility criteria for access to non-public Registration data?
- 1944 ● Do those parties/groups consist of different types of third-party requestors?
- 1945 ● What data elements should each user/party have access to?

1946

1947 In this context, the EPDP team will consider amongst other issues, disclosure in the
1948 course of intellectual property infringement and DNS abuse cases. There is a need to
1949 confirm that disclosure for legitimate purposes is not incompatible with the purposes
1950 for which such data has been collected.

1951

1952 TSG Policy Questions

- 1953
- 1954
- 1955
- 1956
- 1957
- 1958
- 1959
- 1960
- 1961
- 1962
- 1963
- 1964
- 1965
- 1966
- 1967
- 1968
- 1969
- 1970
- 1971
- 1972
- 1973
- 1974
- 1975
- 1976
- 1977
- 1978
- 1979
- 1980
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.²⁰
 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

- 1981 Policy recommendations for a standardised model for lawful disclosure/access of non-
- 1982 public Registration Data
- 1983

GENERAL REQUIRED READING

1984

²⁰ Several noted that this question might not be in scope for the EPDP Team to address.

Description	Link	Requir
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) <ul style="list-style-type: none"> • 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/field_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	

1985

PROPOSED TIMING AND APPROACH

1986

Introduction

1987

Objective of EPDP Team is to develop and agree on policy recommendations for sharing

1988	of non-public Registration Data ²¹ with requesting parties (System for Standardized
1989	Access/Disclosure of Non-Public Registration Data).
1990	
1991	Until legal assurances satisfactory to relevant parties are provided, the development of
1992	the policy recommendations for a System for Standardized Disclosure/Access will be
1993	agnostic to the modalities of the System.
1994	
1995	In parallel, the EPDP Team as a whole should engage with ICANN Org on the
1996	development of policy questions that will help inform the discussions with DPAs which
1997	have as its objective to determine what model of System for Standardized Disclosure
1998	would be fully compliant with GDPR, workable and address/alleviate the legal liability
1999	of contracted parties.
2000	
2001	Non-exhaustive list of topics expected to be addressed:
2002	
2003	◦ Terminology and Working Definitions
2004	◦ Legal guidance needed
2005	◦ Requirements, incl. defining user groups, criteria & criteria/content of request
2006	◦ Publication of process, criteria and content request required
2007	◦ Timeline of process
2008	◦ Receipt of acknowledgment
2009	◦ Accreditation
2010	◦ Authentication & Authorization
2011	◦ Purposes for third party disclosure
2012	◦ Lawful basis for disclosure
2013	◦ Acceptable Use Policy
2014	◦ Terms of use / disclosure agreements, including fulfillment of legal
2015	requirements
2016	◦ Privacy policies
2017	◦ Query policy
2018	◦ Retention and destruction of data
2019	◦ Service level agreements
2020	◦ Financial sustainability
2021	
2022	Approach
2023	
2024	Determine at the outset:
2025	
2026	a) Terminology and working definitions

²¹ 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.

2027 b) Identify legal guidance needed (note, this is also an ongoing activity throughout
2028 all the topics).

2029

2030 Possible logical order to address the remaining topics:

2031

2032 c) Define user groups, criteria and purposes / lawful basis per user group

↓

2033

2034 d) Authentication / authorization / accreditation of user groups

↓

2035

2036 e) Criteria/content of requests per user group

↓

2037

2038 f) Query policy

↓

2039

2040 g) Receipt of acknowledgement, including timeline

↓

2041

2042 h) Response requirements / expectations, including timeline/SLAs

↓

2043

2044 i) Acceptable Use Policy

↓

2045

2046 j) Terms of use / disclosure agreements / privacy policies

↓

2047

2048 k) Retention and destruction of data

2049

2050 l) Overall topic of consideration: financial sustainability

2051

2052 Hereunder further details for each of these topics has been provided. To jump to each
2053 section, please use the links below:

2054

2055 a) [Terminology and Working Definitions](#)

2056

2056 b) [Legal Questions](#)

2057

2057 c) [Define user groups, criteria and purposes / legal basis per user group](#)

2058

2058 d) [Authentication / accreditation of user groups](#)

2059

2059 e) [Format of requests per user group](#)

2060

2060 f) [Query Policy](#)

2061

2061 g) [Receipt of acknowledgement, including timeline](#)

2062

2062 h) [Response requirements / expectations, including timeline / SLAs](#)

2063

2063 i) [Acceptable Use Policy](#)

2064

2064 j) [Terms of use / disclosure agreements / privacy policies](#)

2065

2065 k) [Retention and destruction of data](#)

2066

2066 l) [Financial sustainability](#)

2067

2068 Following the completion of this and other worksheets, each topic (including Phase 1
2069 topics) and its scope of work will form the basis of an overall scheduled work plan.

2070 Some topics may be addressed in parallel, while others may have dependencies to

2071 other work before more informed deliberations can be had. Each topic will be given a
2072 set time to conduct issue deliberations, formulate possible conclusions and or possible
2073 recommendations to the policy questions. Conclusions or recommendations that
2074 obtain a general level of support will advance forward for further consideration and
2075 refinement towards an Initial Report. The goal is to achieve levels of consensus on the
2076 proposal(s) where possible prior to publication.
2077

2078 **a) Topic: Terminology and Working Definitions**

2079

2080 Objective: To ensure that the same meaning is associated with the terms used in the
2081 context of this discussion and avoid confusion, the EPDP Team is to agree on a set of
2082 working definitions. It is understood that these working definitions merely serve to
2083 clarify terminology used, it is in no way intended to restrict the scope of work or
2084 predetermine the outcome. It is understood that these working definitions will need to
2085 be reviewed and revised, as needed, at the end of the process.

2086

2087 Materials to review:

2088

- 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

2089

2090

2091

2092 Related mind map question: None

2093

2094 Related EPDP Phase 1 Implementation: To be confirmed - recommendation #18
2095 implementation may include definitions that may need to be factored into the EPDP
2096 Team's phase 2 deliberations.

2097

2098 Tasks:

2099

- 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)

2100

2101

2102

2103

2104

2105

2106 Target date for completion: 30 May 2019

2107

2108

2109
2110
2111
2112
2113
2114
2115

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
<p>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.</p>	<p>ON HOLD</p> <p>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.</p>	
<p>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)</p>	<p>REWORK</p> <p>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.</p>	
<p>3. Legal guidance should be sought on the possibility of an accreditation-based disclosure system as such. (ISPCP)</p>	<p>ON HOLD</p> <p>The Phase 2 LC has noted this question as premature at this time and will mark the question as “on</p>	

	<p>hold”. The question will be revisited once the EPDP Team has identified the purposes for disclosure.</p>	
<p>4. The question of disclosure to non-EU law enforcement based on Art 6 I f GDPR should be presented to legal counsel. (ISPCP)</p>	<p>REWORK</p> <p>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.</p>	
<p>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)</p>	<p>REWORK</p> <p>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.</p>	

<p>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)</p>	<p>REWORK</p> <p>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.</p>	
<p>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)</p>	<p>REWORK</p> <p>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.</p>	
<p>8. BC Proposes that the EPDP split Purpose 2 into two separate purposes:</p> <ul style="list-style-type: none"> • 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) <p>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</p>	<p>ON HOLD</p> <p>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.</p>	

<p>counsel can make to improve this language? (BC)</p>		
<p>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)</p>	<p>REWORK</p> <p>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.</p>	
<p>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)</p>	<p>REWORK</p> <p>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.</p>	
<p>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)</p>	<p>REWORK</p> <p>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.</p>	
<p>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</p>	<p>REWORK</p>	

<p>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”</p> <p>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:</p> <p>‘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.”</p>	<p>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.</p>	
<p>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:</p> <p>“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.”</p>	<p>REWORK</p> <p>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.</p>	

2116

2117 Tasks:

- 2118 - Determine priority questions for phase 2 related topics
- 2119 - Agree on approach and approval process for questions that emerge throughout
- 2120 deliberations

2121

2122 Target date for completion: Ongoing

2123

2124 **c) Topic: Define user groups, criteria and purposes / lawful basis per user group**

2125

2126 Objective:

2127

- 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.

2128

2129

2130

- Determine purposes and lawful basis per user group for processing data

2131

2132

2133

2134

- 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.

2135

2136

Related mind map questions:

2137

2138

P1-Charter-a

2139

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

2140

2141

a1) Under applicable law, what are legitimate purposes for third parties to access registration data?

2142

2143

a2) What legal bases exist to support this access?

2144

a3) What are the eligibility criteria for access to non-public Registration data?

2145

a4) Do those parties/groups consist of different types of third-party requestors?

2146

2147

Annex to the Temporary Specification:

2148

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

2149

2150

2151

Phase 1 Recommendations

2152

EPDP Team Rec #3

2153

- What are the legitimate purposes for third parties to access registration data?

2154

- What are the eligibility criteria for access to non-public Registration data?

2155

- Do those parties/groups consist of different types of third-party requestors?

2156

2157

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.

2158

2159

2160

2161

2162

2163

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]

2164

2165

2166

2167

2168 *TSG-Final-Q#3*
 2169 3. Describe the general qualifications of a Requestor that is authorized to access non-
 2170 public gTLD domain name registration data, such as which sorts of Requestors get
 2171 access to which fields of non-public gTLD domain name registration data (“the
 2172 authorization policy”).
 2173
 2174 Materials to review:
 2175

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/>

2176

2177 Related EPDP Phase 1 Implementation:

2178 None expected

2179

2180 Tasks:

- 2181 - Develop first list of categories of requestors based on source materials. (Staff)
- 2182 - Review list of categories of requestors and determine eligibility criteria. (All)
- 2183 - Develop abuse types and scenarios to formulate use cases that determine requirements for each requestor
- 2184
- 2185 - Determine purposes and legal basis per user group for processing data (All)
- 2186 - 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)
- 2187
- 2188
- 2189
- 2190 - Confirm all charter questions have been addressed and documented.

2191

2192 Target date for completion: 13 June 2019

2193 (Revisit purpose 2 - once phase 2 work has been completed)

2194

2195

2196 **d) Authentication / authorization / accreditation of user groups**

2197

2198 Objective:

- 2199 - Establish if authentication, authorization and/or accreditation of user groups
2200 should be required
- 2201 - Can an accreditation model compliment or be used with what is
2202 implemented from EPDP-Phase 1 Recommendation #18?
- 2203 - If so, establish policy principles for authentication, authorization and/or
2204 accreditation, including addressing questions such as:
- 2205 - whether or not an authenticated user requesting access to non-public
2206 WHOIS data must provide its legitimate interest for each individual
2207 query/request.
- 2208 - If not, explain why not and what implications this might have on queries from
2209 certain user groups, if any.

2210

2211 Related mind map questions:

2212 *P1-Charter-a/b*

- 2213 (a) Purposes for Accessing Data - What are the unanswered policy questions that
2214 will guide implementation?
- 2215 a7) How can RDAP, that is technically capable, allow Registries/Registrars to
2216 accept accreditation tokens and purpose for the query? Once accreditation
2217 models are developed by the appropriate accreditors and approved by the
2218 relevant legal authorities, how can we ensure that RDAP is technically capable
2219 and is ready to accept, log and respond to the accredited requestor's token?
- 2220 (b) Credentialing – What are the unanswered policy questions that will guide
2221 implementation?
- 2222 b1) How will credentials be granted and managed?
- 2223 b2) Who is responsible for providing credentials?
- 2224 b3) How will these credentials be integrated into registrars'/registries' technical
2225 systems?

2226

2227 *Annex to the Temporary Specification*

- 2228 1. Pursuant to Section 4.4, continuing community work to develop an
2229 accreditation and access model that complies with GDPR, while recognizing the need to
2230 obtain additional guidance from Article 29 Working Party/European Data Protection
2231 Board.

2232

2233 *TSG-Final-Q#2*

- 2234 Identify and select Identity Providers (if that choice is made) that can grant credentials
2235 for use in the system.

2236

2237 Materials to review:

2238

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	

2239

2240 Related EPDP Phase 1 Implementation:

2241 None expected.

2242

2243 Tasks:

- 2244 ● Review materials listed above and discuss perspectives on authentication /
- 2245 authorization.(EPDP)
- 2246 ● Confirm definitions of key terms Authorization, Accreditation and
- 2247 Authentication
- 2248 ● Determine full list of policy questions and deliberate each
- 2249 ● Determine possible solutions or proposed recommendation, if any
- 2250 ● Confirm all charter questions have been addressed and documented

2251

2252 Target date for completion: ICANN 65

2253

2254

2255 **e) Criteria / content of requests per user group**

2256

2257 Objective: establish minimum policy requirements, criteria and content for requests
 2258 per user group as identified under c.

2259

2260 Related mind map questions:

2261

2262 *P1-Charter-c*

2263 c1) What rules/policies will govern users' access to the data?

2264

2265 Materials to review:

2266

Description	Link	Required because
<ul style="list-style-type: none"> 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/Domainsdate nanfrage/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	

2267

2268 Related EPDP Phase 1 Implementation:

2269

2270 Recommendation #18 (but does NOT require automatic disclosure of information)

2271

2272 Minimum Information Required for Reasonable Requests for Lawful Disclosure:

2273

- 2274 ● Identification of and information about the requestor (including, the
2275 nature/type of business entity or individual, Power of Attorney statements,
2276 where applicable and relevant);
- 2277 ● Information about the legal rights of the requestor and specific rationale and/or
2278 justification for the request, (e.g. What is the basis or reason for the request;
2279 Why is it necessary for the requestor to ask for this data?);
- 2280 ● Affirmation that the request is being made in good faith;
- 2281 ● A list of data elements requested by the requestor and why this data is limited
2282 to the need;
- 2283 ● Agreement to process lawfully any data received in response to the request.

2283

2284 Tasks:

2285

- 2286 ● Confirm implementation approach for recommendation #18
- 2287 ● Confirm definitions of key terms
- 2288 ● Determine full list of policy questions and deliberate each
- 2289 ● Determine possible solutions or proposed recommendation, if any
- 2290 ● Confirm all charter questions have been addressed and documented

2290

2291 Target date for completion: ICANN 65

2292

2293 **f) Query policy**

2294

2295 Objective: Establish minimum policy requirements for logging of queries, defining the
2296 appropriate controls for when query logs should be made available, and if there should
2297 be query limitations for authenticated and unauthenticated users of the SSAD.

2298

- 2299 ● How will access to non-public registration data be limited in order to minimize
2300 risks of unauthorized access and use (e.g. by enabling access on the basis of
2301 specific queries only as opposed to bulk transfers and/or other restrictions on
2302 searches or reverse directory services, including mechanisms to restrict access
2303 to fields to what is necessary to achieve the legitimate purpose in question)?
- 2304 ● Should confidentiality of queries be considered, for example by law
2305 enforcement?
- 2306 ● How should query limitations be balanced against realistic investigatory cross-
2307 referencing needs?

2308

2309 Related mind map questions:

2310

2311 *P1-Charter-a*

2312 a7) How can RDAP, that is technically capable, allow Registries/Registrars to accept
 2313 accreditation tokens and purpose for the query? Once accreditation models are
 2314 developed by the appropriate accreditors and approved by the relevant legal
 2315 authorities, how can we ensure that RDAP is technically capable and is ready to accept,
 2316 log and respond to the accredited requestor's token?

2317

2318 *Annex to the Temporary Specification:*

2319 6 Limitations in terms of query volume envisaged under an accreditation program
 2320 balanced

2321 against realistic investigatory cross-referencing needs.

2322 7 Confidentiality of queries for Registration Data by law enforcement authorities.

2323

2324 Materials to review:

2325

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.

2326

2327 Related EPDP Phase 1 Implementation: None.

2328

2329 Tasks:

- 2330 ● Confirm definitions of key terms
- 2331 ● Determine full list of policy questions and deliberate each
- 2332 ● Determine possible solutions or proposed recommendation, if any
- 2333 ● Confirm all charter questions have been addressed and documented

2334

2335 Target date for completion: ICANN 65

2336

2337 **g) Receipt of acknowledgement, including timeline**

2338

2339 Objective: Define policy requirements around timeline of acknowledgement of receipt
 2340 and additional requirements (if any) the acknowledgement should contain.

2341

2342 What, if any, are the baseline minimum standardized receipt of acknowledgement
 2343 requirements for registrars/registries? What about 'urgent' requests and how are these
 2344 defined?

2345

2346 Related mind map questions:

2347

2348 *P1-Charter-c*
 2349 c1) What rules/policies will govern users' access to the data?

2350
 2351 Materials to review:
 2352

Description	Link	Required because
Phase 1 Final Report Rec. 18 Timeline & Criteria for Registrar and Registry Operator Responses	https://gns0.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf p. 19	

2353
 2354 Related EPDP Phase 1 Implementation: - Recommendation #18:
 2355 Timeline & Criteria for Registrar and Registry Operator Responses_-
 2356 Registrars and Registries must reasonably consider and accommodate requests for
 2357 lawful disclosure:
 2358 • Response time for acknowledging receipt of a Reasonable Request for Lawful
 2359 Disclosure. Without undue delay, but not more than two (2) business days from
 2360 receipt, unless shown circumstances does not make this possible.

2361
 2362 Tasks:
 2363 • Confirm definitions of key terms
 2364 • Determine full list of policy questions and deliberate each
 2365 • Determine possible solutions or proposed recommendation, if any
 2366 • Confirm all charter questions have been addressed and documented

2367
 2368 Target date for completion: TBD
 2369

2370 **h) Response requirements / expectations, including timeline/SLAs**

2371
 2372 Objective: Define policy requirements around response requirements, including
 2373 addressing questions such as:

2374
 2375 - including addressing questions such as:
 2376 - Whether or not full WHOIS data must be returned when an
 2377 authenticated user performs a query.
 2378 - What should be the SLA commitments for responses to requests for
 2379 access/disclosure

- 2380 - What are the minimum requirements for responses to requests,
- 2381 including denial of requests?

- 2382 Related mind map questions:
- 2383
- 2384 *P1-Charter-a/c*
- 2385 a5) What data elements should each user/party have access to based on their purpose?
- 2386 a6) To what extent can we determine a set of data elements and potential scope
- 2387 (volume) for specific third
- 2388 parties and/or purposes?
- 2389 c1) What rules/policies will govern users' access to the data?
- 2390
- 2391 *Phase 1 Recommendation - #3*
- 2392 What data elements should each user/party have access to?
- 2393
- 2394 *Annex to the Temporary Specification*
- 2395 2. Addressing the feasibility of requiring unique contacts to have a uniform anonymized
- 2396 email address across domain name registrations at a given Registrar, while ensuring
- 2397 security/stability and meeting the requirements of Section 2.5.1 of Appendix A.
- 2398
- 2399 *TSG-Final-Q#6*
- 2400 Describe service Level Requirements (SLRs) for each component of the system,
- 2401 including whether those SLRs and evaluations of component operators against them
- 2402 are made public, and for handling complaints about access.
- 2403 *TSG-Final-Q#7*
- 2404 Specify legitimate causes for denying a request.
- 2405 *TSG-Final-Q#8*
- 2406 Outline support for correlation via a pseudonymity query as described in Section 7.2.
- 2407
- 2408 Materials to review:
- 2409

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	

<p>Final Report on the Privacy & Proxy Services Accreditation Issues (7 December 2015)</p> <ul style="list-style-type: none"> Annex B – Illustrative Disclosure Framework applicable to Intellectual Property Rights-holder Disclosure Requests – pages 90 - 92 	<p>https://gns0.icann.org/sites/default/files/efield_48305/ppsai-final-07dec15-en.pdf</p>	<p>Section of PPSAI illustrative disclosure framework detailing required minimum response</p>
--	--	---

2410

2411 Related EPDP Phase 1 Implementation:

2412 Recommendation #18:

- 2413 ● Requirements for what information responses should include. Responses where
2414 disclosure of data (in whole or in part) has been denied should include:
2415 rationale sufficient for the requestor to understand the reasons for the
2416 decision, including, for example, an analysis and explanation of how the
2417 balancing test was applied (if applicable).
- 2418 ● Logs of Requests, Acknowledgements and Responses should be maintained in
2419 accordance with standard business recordation practices so that they are
2420 available to be produced as needed including, but not limited to, for audit
2421 purposes by ICANN Compliance;
- 2422 ● Response time for a response to the requestor will occur without undue delay,
2423 but within maximum of 30 days unless there are exceptional circumstances.
2424 Such circumstances may include the overall number of requests received. The
2425 contracted parties will report the number of requests received to ICANN on a
2426 regular basis so that the reasonableness can be assessed.
- 2427 ● A separate timeline of [less than X business days] will considered for the
2428 response to ‘Urgent’ Reasonable Disclosure Requests, those Requests for which
2429 evidence is supplied to show an immediate need for disclosure [time frame to
2430 be finalized and criteria set for Urgent requests during implementation].

2431

2432 Tasks:

- 2433 ● Confirm definitions of key terms
- 2434 ● Determine full list of policy questions and deliberate each
- 2435 ● Determine possible solutions or proposed recommendation, if any
- 2436 ● Confirm all charter questions have been addressed and documented

2437

2438 Target date for completion: August

2439

2440 **i) Acceptable Use Policy**

2441

2442 Objective: Define the policy requirements around:

2443

- 2444 1. How should a code of conduct (if any) be developed, continuously evolve
- 2445 and be enforced?
- 2446 2. If ICANN and its contracted parties develop a code of conduct for third
- 2447 parties with legitimate interest, what features and needs should be considered?
- 2448 3. Are there additional data flows that must be documented outside of what
- 2449 was documented in Phase 1?
- 2450 Can a Code of Conduct model compliment or be used with what is implemented
- 2451 from EPDP-Phase 1 Recommendation #18?

2452

2453 Related mind map questions:

2454

2455 *P1-Charter-c*

2456 c1) What rules/policies will govern users' access to the data?

2457 c2) What rules/policies will govern users' use of the data once accessed?

2458 c3) Who will be responsible for establishing and enforcing these rules/policies?

2459 c4) What, if any, sanctions or penalties will a user face for abusing the data, including

2460 future

2461 restrictions on access or compensation to data subjects whose data has been abused in

2462 addition to any sanctions already provided in applicable law?

2463 c5) What kinds of insights will Contracted Parties have into what data is accessed and

2464 how it is used?

2465 c6) What rights do data subjects have in ascertaining when and how their data is

2466 accessed and used?

2467 c7) How can a third party access model accommodate differing requirements for data

2468 subject notification of data disclosure?

2469

2470 Materials to review:

2471

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	

2472

2473 Related EPDP Phase 1 Implementation: None.

2474

2475 Tasks:

- 2476 ● Determine full list of policy questions and deliberate each
- 2477 ● Determine possible solutions or proposed recommendation, if any
- 2478 ● Confirm all charter questions have been addressed and documented

2479

2480 Target date for completion: August

2481

2482 **j) Terms of use / disclosure agreements / privacy policies**

2483

2484 Objective: Define policy requirements around terms of use for third parties who seek to
 2485 access nonpublic registration data:

2486

- 2487 ● At a minimum, what required measures are needed to adequately safeguard personal data that may be made available to an accredited user/third party?
- 2488 ● What procedures should be established for accessing data?
- 2489 ● What procedures should be established for limiting the use of data that is properly accessed?
- 2490 ● Should separate Terms of Use be required for different user groups?
- 2491 ● Who would monitor and enforce compliance with Terms of Use?

2492

2493

2494

- 2495 • What mechanism would be used to require compliance with the Terms
2496 of Use?

2497

2498 Related mind map questions:

2499

2500 *P1-Charter-c*

2501 c1) What rules/policies will govern users' access to the data?

2502 c2) What rules/policies will govern users' use of the data once accessed?

2503 c3) Who will be responsible for establishing and enforcing these rules/policies?

2504 c4) What, if any, sanctions or penalties will a user face for abusing the data, including
2505 future

2506 restrictions on access or compensation to data subjects whose data has been abused in
2507 addition to any sanctions already provided in applicable law?

2508

2509 *TSG-Final-Q#4*

2510 Detail whether a particular category of Requestors or Requestors in general, can
2511 download logs of their activity.

2512 *TSG-Final-Q#10*

2513 Describe the conditions, if any, under which requests would be disclosed to CPs.

2514 *TSG-Final-Q#11*

2515 Provide legal analysis regarding liability of the operators of various components of the
2516 system.

2517 *TSG-Final-Q#12*

2518 Outline a procedure for fielding complaints about inappropriate disclosures and,
2519 accordingly, an Acceptable Use Policy

2520

2521 Materials to review:

2522

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	

2523

2524 Related EPDP Phase 1 Implementation:

2525

2526 Tasks:

- 2527 • Confirm definitions of key terms

- 2528 ● Determine full list of policy questions and deliberate each
- 2529 ● Determine possible solutions or proposed recommendation, if any
- 2530 ● Confirm all charter questions have been addressed and documented

2531
 2532 Target date for completion: September

2533
 2534 **k) Retention and destruction of data**

2535
 2536 Objective: Establish minimum policy requirements for retention, deletion and logging
 2537 of data retained for parties involved in the SSAD, including but limited to, gTLD
 2538 registration data, user account information, transaction logs, and metadata such as
 2539 date-and-time of requests

2540
 2541 Related mind map questions:

2542
 2543 *P1-Charter-c*
 2544 c2) What rules/policies will govern users' use of the data once accessed?

2545
 2546 *TSG-Final-Q#5*
 2547 Describe data retention requirements imposed on each component of the system.

2548
 2549 Materials to review:
 2550

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	

2551
 2552 Related EPDP Phase 1 Implementation: Recommendation #15:
 2553 1. In order to inform its Phase 2 deliberations, the EPDP team recommends that ICANN
 2554 Org, as a matter of urgency, undertakes a review of all of its active processes and

2555 procedures so as to identify and document the instances in which personal data is
2556 requested from a registrar beyond the period of the 'life of the registration'. Retention
2557 periods for specific data elements should then be identified, documented, and relied
2558 upon to establish the required relevant
2559 and specific minimum data retention expectations for registrars. The EPDP Team
2560 recommends community members be invited to contribute to this data gathering
2561 exercise by providing input on other legitimate purposes for which different retention
2562 periods may be applicable.

2563
2564 2. In the interim, the EPDP team has recognized that the Transfer Dispute Resolution
2565 Policy ("TDRP") has been identified as having the longest justified retention period of
2566 one year and has therefore recommended registrars be required to retain only those
2567 data elements deemed necessary for the purposes of the TDRP, for a period of fifteen
2568 months following the life of the registration plus three months to implement the
2569 deletion, i.e., 18 months. This retention is grounded on the stated policy stipulation
2570 within the TDRP that claims under the policy may only be raised for a period of 12
2571 months after the alleged breach (FN: see TDRP section 2.2) of the Transfer Policy (FN:
2572 see Section 1.15 of TDRP). This retention period does not restrict the ability of
2573 registries and registrars to retain data elements provided in Recommendations 4 -7 for
2574 other purposes specified in Recommendation 1 for shorter periods.

2575
2576 3. The EPDP team recognizes that Contracted Parties may have needs or requirements
2577 for different retention periods in line with local law or other requirements. The EPDP
2578 team notes that nothing in this recommendation, or in separate ICANN-mandated
2579 policy, prohibits contracted parties from setting their own retention periods, which
2580 may be longer or shorter than what is specified in ICANN policy.

2581
2582 4. The EPDP team recommends that ICANN Org review its current data retention
2583 waiver procedure to improve efficiency, request response times, and GDPR
2584 compliance, e.g., if a Registrar from a certain jurisdiction is successfully granted a data
2585 retention waiver, similarly-situated Registrars might apply the same waiver through a
2586 notice procedure and without having to produce a separate application.

2587
2588 Tasks:

- 2589 ● Confirm definitions of key terms
- 2590 ● Determine full list of policy questions and deliberate each
- 2591 ● Determine possible solutions or proposed recommendation, if any
- 2592 ● Confirm all charter questions have been addressed and documented

2593
2594 Target date for completion: September

2595
2596

2597 **I) Financial sustainability**

2598

2599 Objective: Ensure that all aspects of SSAD are financially sustainable. Consider how and
 2600 by whom costs of SSAD implementation and management are borne.

- 2601 ● Determine if market inefficiencies existed prior to May 2018 and if any exist in a
 2602 post EPDP-Phase 1 implemented world.
- 2603 ● Should contracted parties and or ICANN bear the cost of a standardized
 2604 solution, even if the disclosure of registration data is considered in the public
 2605 interest?
- 2606 ● If accreditation is a viable solution, should there be application fees associated,
 2607 or should a fee structure be based on the type (tiered), size, or quantify of
 2608 disclosures?
- 2609 ● Should or could data subjects be compensated for disclosures of their data?

2610

2611 Related mind map questions: None

2612

2613 Materials to review:

2614

Description	Link	Required because

2615

2616 Related EPDP Phase 1 Implementation: None

2617

2618 Tasks:

- 2619 ● Confirm definitions of key terms
- 2620 ● Determine full list of policy questions and deliberate each
- 2621 ● Determine possible solutions or proposed recommendation, if any
- 2622 ● Confirm all charter questions have been addressed and documented

2623

2624 Target date for completion: TBD

2625

2626

2627

Annex B – General Background

2628

Process & Issue Background

2629

2630

2631

2632

2633

2634

2635

2636

2637

2638

2639

2640

2641

2642

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](#).

2643

○ Issue Background

2644

2645

2646

2647

2648

2649

2650

2651

2652

2653

2654

2655

2656

2657

2658

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".²² 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.

2659

2660

2661

2662

2663

2664

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

²² See section 3.1(a) of the Registry Agreement: <https://www.icann.org/resources/unthemed-pages/org-agmt-html-2013-09-12-en>

2665 Governmental Advisory Committee (GAC), the Country Code Supporting Organization
2666 (ccNSO), the At-Large Advisory Committee (ALAC), the Root Server System Advisory
2667 Committee (RSSAC) and the Security and Stability Advisory Committee (SSAC) were
2668 each been invited to appoint up to a set number of members and alternates, as
2669 outlined in the [charter](#). In addition, the ICANN Board and ICANN Org have been invited
2670 to assign a limited number of liaisons to this effort.

2671
2672 The EPDP Team published its Phase 1 Initial Report for [Public Comment](#) on 21
2673 November 2018. The EPDP Team incorporated public comments into its Phase 1 [Final](#)
2674 [Report](#), and the GNSO Council voted to adopt all 29 recommendations within the
2675 EPDP’s Phase 1 [Final Report](#) at its meeting on 4 March 2019. On 15 May 2019, the
2676 ICANN Board [adopted](#) the EPDP Team’s Phase 1 Final Report, with the exception of
2677 parts of two recommendations: 1) Purpose 2 in Recommendation 1 and 2) the option
2678 to delete data in the Organization field in Recommendation 12. As per the ICANN
2679 Bylaws, a consultation will take place between the GNSO Council and the ICANN Board
2680 to discuss the parts of the EPDP Phase 1 recommendations that were not adopted by
2681 the ICANN Board. At the same time, an Implementation Review Team (IRT), consisting
2682 of the ICANN organization (ICANN org) and members of the ICANN community, will
2683 now implement the approved recommendations of the EPDP Team’s Phase 1 Final
2684 Report. For further details on the status of implementation, please see [here](#).

2685
2686 On 2 May 2019, the EPDP Team begun Phase 2 of its work. The scope for EPDP Phase 2
2687 includes (i) discussion of a system for standardized access/disclosure to nonpublic
2688 registration data, (ii) issues noted in the [Annex to the Temporary Specification for gTLD](#)
2689 [Registration Data](#) (“Important Issues for Further Community Action”), and (iii) issues
2690 deferred from Phase 1, e.g., legal vs natural persons, redaction of city field, et. al. For
2691 further details, please see [here](#).

2692
2693
2694

2695

Annex C – EPDP Team Membership and Attendance

2696

EPDP Team Membership and Attendance

2697

2698

The members of the EPDP Team are:

	Members / Liaisons²³	Affiliation	SOI	% of Meetings Attended²⁴
1	Alan Woods	RySG	SOI	
2	Matthew Crossman	RySG	SOI	
3	Marc Anderson	RySG	SOI	
4	James M. Bladel	RrSG	SOI	
5	Matt Serlin	RrSG	SOI	
6	Volker Greimann	RrSG	SOI	
7	Alex Deacon	IPC	SOI	
8	Brian King	IPC	SOI	
9	Margie Milam	BC	SOI	
10	Mark Svancarek	BC	SOI	
11	Fiona Assonga	ISPCP	SOI	
12	Thomas Rickert	ISPCP	SOI	
13	Stephanie Perrin	NCSG	SOI	
14	Ayden Férdeline	NCSG	SOI	
15	Milton Mueller	NCSG	SOI	
16	Julf Helsingius	NCSG	SOI	
17	Amr Elsadr	NCSG	SOI	
18	Farzaneh Badiei	NCSG	SOI	

²³ For historic data on members / alternates, please see <https://community.icann.org/x/3JUzBw>.

²⁴ This does not include attendance to F2F meetings which is recorded separately. See <https://community.icann.org/x/6oECBw>, <https://community.icann.org/x/WgVxBw>.

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

2699
2700

The alternates of the EPDP Team are:

	Alternate	Affiliation	SOI	% of Meetings Attended
1	Beth Bacon	RySG	SOI	
2	Arnaud Wittersheim	RySG	SOI	
3	Sean Baseri	RySG	SOI	
4	Owen Smigelski	RrSG	SOI	
5	Sarah Wyld	RrSG	SOI	
6	Theo Geurts	RrSG	SOI	

7	Jennifer Gore	IPC	SOI	
8	Steve DelBianco	BC	SOI	
9	Suman Lal Pradhan	ISPCP	SOI	
10	Tatiana Tropina	NCSG	SOI	
11	David Cake	NCSG	SOI	
12	Stefan Filipovic	NCSG	SOI	
13	Olga Cavalli	GAC	SOI	
14	Rahul Gosain	GAC	SOI	
15	TBD	GAC		
16	Holly Raiche	ALAC	SOI	
17	Bastiaan Goslings	ALAC	SOI	
18	Tara Whalen	SSAC	SOI	
19	Rod Rasmussen	SSAC	SOI	

2701

2702 The detailed attendance records can be found at

2703 <https://community.icann.org/x/4opHBQ>.

2704

2705 The EPDP Team email archives can be found at [https://mm.icann.org/pipermail/gnso-](https://mm.icann.org/pipermail/gnso-epdp-team/)2706 [epdp-team/](https://mm.icann.org/pipermail/gnso-epdp-team/).

2707

2708 * The following are the ICANN SO/ACs and GNSO Stakeholder Groups and

2709 Constituencies for which EPDP TEAM members provided affiliations:

2710 RrSG – Registrar Stakeholder Group

2711 RySG – Registry Stakeholder Group

2712 BC – Business Constituency

2713 NCSG – Non-Commercial Stakeholder Group

2714 IPC – Intellectual Property Constituency

2715 ISPCP – Internet Service and Connection Providers Constituency

2716 GAC – Governmental Advisory Committee

2717 ALAC – At-Large Advisory Committee

2718 SSAC – Security and Stability Advisory Committee

2719

Annex D - Community Input

2720

Request for Input

2721

2722

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:

2729

2730

- The GNSO Business Constituency (BC)

2731

- The GNSO Non-Commercial Stakeholder Group (NCSG)

2732

- The Registries Stakeholder Group (RySG)

2733

- The Registrar Stakeholder Group (RrSG)

2734

- The Internet Service Providers and Connectivity

2735

- Providers Constituency (ISPCP)

2736

2737

The full statements can be found here: <https://community.icann.org/x/zlWGBg>.

2738

Review of Input Received

2739

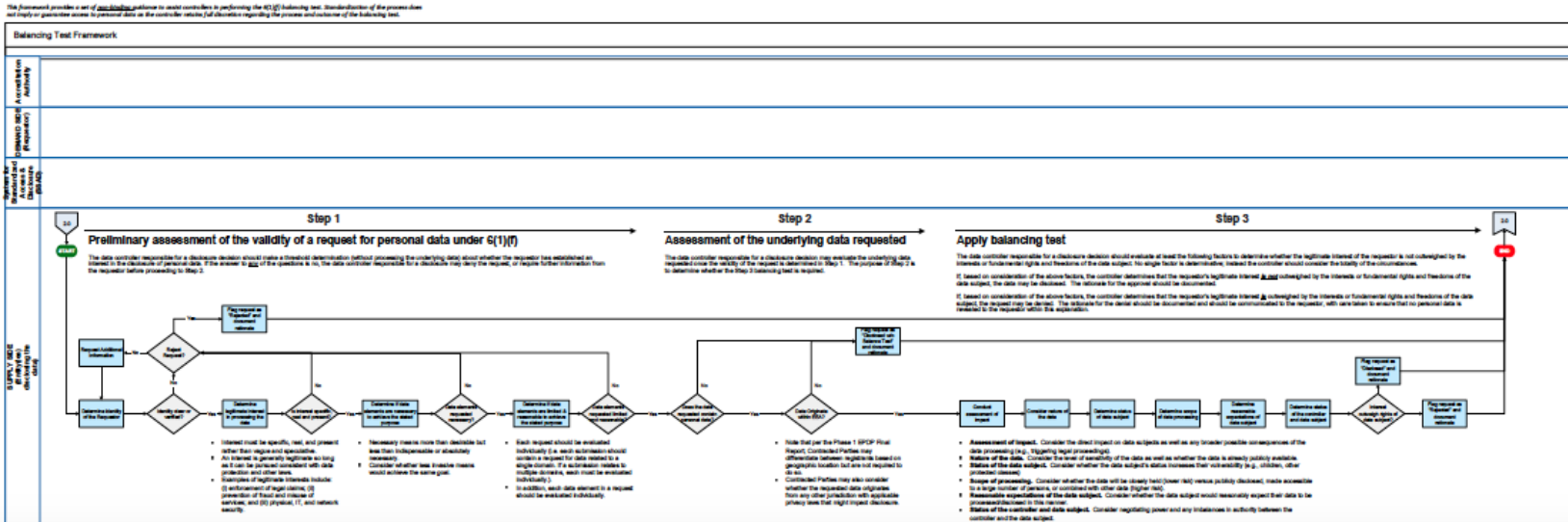
2740

All of the input received was added to the [Early Input review tool](#) and considered by the EPDP Team.

2741

Annex E - Balancing Test Framework

See [here](#) for standalone file



Annex F – Legal Committee

Phase 2 Questions Submitted to Bird & Bird

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

Further, assume the following safeguards are in place

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

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

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 eliminate¹ this risk?
3. In this scenario, would the CP be a controller or a processor², 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:
 - o represents that it has a lawful basis for requesting and processing the data,
 - o provides its lawful basis,
 - o represents that it is requesting only the data necessary for its purpose,
 - o agrees to process the data in accordance with GDPR, and
 - o 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 1 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 1 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 1 c GDPR).

c. In the light of this, 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?

- [Executive Summaries](#)²⁵

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

²⁵ 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 Jehovah's Witnesses 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 case²⁶ (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)

²⁶ 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 GDPR’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 situations, 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:
 - o represents that it has a lawful basis for requesting and processing the data,
 - o provides its lawful basis,
 - o represents that it is requesting only the data necessary for its purpose,
 - o agrees to process the data in accordance with GDPR, and
 - o 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 eliminate²⁷¹ this risk?
 - c. In this scenario, would the CP be a controller or a processor²⁸², 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?

²⁷ "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

²⁸https://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).²⁹
- 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

²⁹ 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).