
Public Comment Summary Report

Registration Data Consensus Policy for gTLDs

Open for Submissions Date:

Wednesday, 24 August 2022

Closed for Submissions Date:

Monday, 05 December 2022 (Extended from Monday, 31 October 2022)

Summary Report Due Date:

Friday, 20 January 2023 (Extended from Wednesday, 30 November 2022)

Category: Policy

Requester: ICANN org

ICANN org Contact(s): globalsupport@icann.org

Open Proceeding Link:

<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022>

Outcome:

ICANN org received a total of fourteen (14) submissions. The comments were categorized into the following categories: (1) comments suggesting that the draft policy language requires additional clarifications, (2) comments suggesting that the draft policy language does not accurately reflect the EPDP phase 1 policy recommendations, (3) comments identifying additional concerns or issues in the draft policy language, (4) general comments, and (5) comments suggesting the proposed redlines made to redlined policies and procedures are inaccurate. This Public Comment summary report includes an ICANN org staff summary of the comments and observations on the topic. ICANN org will consider the input received and will collaborate with the Implementation Review Team (IRT) to update relevant information to the Draft Registration Data Consensus Policy and existing policies and procedures impacted by the Registration Data Consensus Policy.

Section 1: What We Received Input On

During the Public Comment proceeding, ICANN org received 14 comments on two different public comment forums from organizations, groups, and individuals. Comments were on the draft Registration Data Consensus Policy for gTLDs, which sets out Consensus Policy requirements concerning the collection, transfer, and publication of gTLD registration data and the updates to existing policies and procedures impacted by the Registration Data Policy.

ICANN org will consider the input received and will collaborate with the IRT to update relevant information on the topic. ICANN org values the opportunity to receive comments from the ICANN community and thanks those who participated in this proceeding.

Section 2: Submissions

Organizations and Groups:		
Name	Submitted by	Initials
Registrar Stakeholder Group	Zoe Bonython	RrSG
Registries Stakeholder Group		RySG
Business Constituency		BC
Governmental Advisory Committee	Fabien Betremieux	GAC
At-Large Advisory Committee		ALAC
Internet Infrastructure Coalition		i2C
Cross-Community Working Party on ICANN and Human Rights	Ephraim Percy Kenyanito	CCWP-HR
Intellectual Property Constituency	Brian King	IPC
International Trademark Association		INTA

Individuals:		
Name	Affiliation (if provided)	Initials
Tucows	RrSG	
Werner Staub	CORE Association	
Lucien Castex	AFNIC	
Eric Rokobauer	Newfold Digital, Inc.	
Imran Hossen	Business Constituency	

Section 3: Summary of Submissions

There were 14 submissions to the Public Comment Proceeding. For the purpose of this summary, key themes from the comments received are in bold below. All 14 comments that were received are available on the Public Comment page.

Comments suggesting the following sections in the Registration Data Policy require Additional Clarifications.

Nine groups or organizations provided comments suggesting the following areas within the drafted policy language require additional clarification.

Section 2:

-
1. “The GAC notes that Section 2.2 of the Draft Policy stipulates that “*Registrar Operator’s and Registrar’s Processing of Personal Data contained in Registration Data for purposes other than the purposes identified in the Data Protection Agreement required by Section 5 is beyond the scope of this Policy*”. The GAC recommends **clarifying this language as it is unclear what “other purposes” includes**. This is especially relevant given that Data Protection Agreements in Section 5 are made conditional on an assessment by contracted parties and **the lack of a common model for data processing agreements makes it unclear what purposes could be covered therein.**” (GAC)

<https://gac.icann.org/statement/public/gac-comments-registration-data-consensus-policy-21nov22.pdf>

2. “The expression “**other purposes**” should be further clarified to identify what purposes would be covered under section 2.2” (AFNIC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/afnic-21-11-2022>

Section 3:

1. “Unless there is a compelling reason, **all definitions in the policy should reside in this section**. For example, Section 9.2.2. Defines “Redact”, and Implementation Note H defines “Creation Date”. **For clarity, these definitions should be moved to Section 3.**” (RySG) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/rysg-registries-stakeholder-group-21-11-2022>

Section 5:

1. “The RrSG notes that ICANN has been negotiating a DPA with the contracted parties for several years. The **RrSG encourages ICANN to complete these negotiations** and to sign the respective DPAs with registrars and registries. Additionally, the RrSG notes that the **wording in this section is ambiguous. The recommendation does not specify who can request a DPA, so theoretically a third party can require their own DPA. The recommendation should be clarified to ensure that registrars are not required to negotiate and/or sign substantial DPAs relating to their ICANN accreditation.** If it is anticipated that there may be additional DPAs with third parties, then the RrSG recommends that the contracted parties create a standard DPA that can be used.”

(RrSG) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/rrsg-21-11-2022>

2. “The section should be **clarified** in particular **with regard to the obligation for the parties to “enter into required data protection agreements”**, either under applicable law or the aforementioned policy recommendations. (AFNIC)

<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/afnic-21-11-2022>

-
3. **“Newfold Digital supports the statement made by the RrSG in their Public Comment.** Preferred to have had the respective DPAs between ICANN and registrars and registries completed in tandem with providing public comment to the policy language. **Encourage ICANN to complete these negotiations.” (Newfold Digital)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/newfold-digital-inc-28-11-2022>

Section 6:

1. “The RySG is aware that the **global legislative environment continues to evolve** and believes that **a slight addition to Section 6.7 would add clarity** to what is allowable as part of this section. Suggested amendment (additional text between **): **6.7. Registrar MAY collect additional data elements as required by its Registry-Registrar Agreement and/or the Registry Operator’s Registration Policy**, **including if required by law**.”(RySG) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/rysg-registries-stakeholder-group-21-11-2022>
2. “The RrSG notes that **recommendation 6.3 applies only at the time of registration**, and suggests that **to ensure PII is not inadvertently disclosed publicly**, that **these requirements also apply when technical contact information is updated**. The RrSG is also concerned that **registrars** may not have a direct relationship with the technical contact, and **may not be able to properly obtain consent to display PII**. The IRT should resolve this ambiguity.”(RrSG) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/rrsg-21-11-2022>
3. “With respect to **6.5.1. Registrant Organization**, the following note should be added: “In the absence of a separate dedicated field available for a unique Public Identifier, as in Section 4.8 of RFC 7483, for the unequivocal identification of the registrant, **the registrar MUST allow the registrant to optionally append its public identifier to the Registrant Organization data element**. It will then take the form of URI separated by a single space from the name. If a public identifier URI is added, it is regarded as an identity claim made in the registration.” [URI name spaces appropriate to the identification of registrants include the Legal Entity Identifiers URN name space starting with 'urn:lei:' and the Global Location Identifiers URN name space starting with 'urn:epc:id:sgln:'. In future, Decentralized Identifiers whose URIs start with "did:" may gain acceptance as appropriate registrant identifiers. See:
 - a. <https://www.rfc-editor.org/rfc/rfc7483#section-4.8> for publicId
 - b. <https://www.iana.org/assignments/urn-namespaces/urn-namespaces.xhtml> under LEI and RFC5134 for relevant URN name spaces
 - c. <https://www.w3.org/TR/did-spec-registries/> for DID methods.”(CORE Association) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/staub-werner-21-11-2022>

Section 7:

1. “The RrSG notes that while recommendation 7.2 refers to “Registrar Whois Server”, concurrently **the RA and RAA are being amended to primarily replace whois obligations with RDAP requirements.** While registrars may continue to provide whois service after the transition from whois to RDAP, **the recommendations should include a reference to this change to avoid future ambiguity.”(RrSG)**
<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/rrsg-21-11-2022>
2. Further clarification is needed regarding the obligation to have a Data Processing Agreement (**AFNIC**) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/afnic-21-11-2022>
3. “With respect **7.4.1. Registrant Organization, the following note should be added:** “In the absence of a separate dedicated field available for a unique Public Identifier made available by the registry, as in Section 4.8 of RFC 7483, for the unequivocal identification of the registrant, **the registrar MAY append the registrant's public identifier to the Registrant Organization data element.** It will then take the form of URI separated by a single space from the name. If a public identifier URI is added, it is regarded as an identity claim made in the registration.” [URI name spaces appropriate to the identification of registrants include the Legal Entity Identifiers URN name space starting with 'urn:lei:' and the Global Location Identifiers URN name space starting with 'urn:epc:id:sgln:'. In future, Decentralized Identifiers whose URIs start with "did:" may gain acceptance as appropriate registrant identifiers. See
 - a. <https://www.rfc-editor.org/rfc/rfc7483#section-4.8> for publicId,
 - b. <https://www.iana.org/assignments/urn-namespaces/urn-namespaces.xhtml> under [LEI and RFC5134](#) for relevant URN name spaces
 - c. <https://www.w3.org/TR/did-spec-registries/> for DID methods.]” (**CORE Association**) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/staub-werner-21-11-2022>

Section 9:

1. “For clarity, **9.2.1. should be separated into two separate sections** as follows:
(additional text between **) **9.2.1: Registry Operator and Registrar MUST apply the** (deleted text: [following requirements]) ****requirements of this Section 9** in RDDS if redaction of Personal Data contained in Registration Data is required in order to comply with applicable laws. 9.2.2: **Where redaction of Personal Data contained in Registration Data is not required by law,** Registry Operator and Registrar MAY apply the (deleted text: [following requirements]) ****requirements of this Section 9** IF (i) they have a commercially reasonable purpose to do so; OR (ii) where it is not technically feasible to limit application of the requirements of this section. In determining whether to apply the following requirements, Registry Operator and****

Registrar MAY, but are not required to, consider (i) whether Registration Data pertains to a legal person or contains Personal Data; and (ii) the geographic location of the Registered Name Holder or relevant contact.” (RySG)

<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/rysg-registries-stakeholder-group-21-11-2022>

Section 10:

1. **“Section 10. Requires “Registrar and Registry Operator MUST publish on their homepage a direct link to a page where the mechanism and process for submitting Disclosure Requests is Detailed”.** The relevant source recommendation, Recommendation 18, refers to the fact that “Registrars and Registry Operators must publish, in a publicly accessible section of their website, the mechanism and process for submitting Reasonable Requests for Lawful Disclosure”. **The policy recommendations deliberately do not use the word “homepage” as this is not always the best or most appropriate place to provide the link. Some flexibility should be given to Registrars and Registry operators to make that determination.”** (RySG)
<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/rysg-registries-stakeholder-group-21-11-2022>
2. **“10.6 uses the ambiguous term “business days” and should rather specify that it is the registrar’s business days that are relevant. Tucows’ Recommended Language for Section 10: *For Urgent Requests for Lawful Disclosure, Registrar and Registry Operator MUST acknowledge and respond without undue delay, but no more than two (2) business days (as determined by the recipient) from receipt.*”** (Tucows) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/tucows-14-10-2022>

Section 12:

1. “Rec #15 arrived at 18 months as an “interim” retention period. **The final determination of retention period may be longer, based on legitimate purposes** identified through community consultation.” (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

Addendum I:

1. “While **this section** accurately reflects the Policy Recommendation language, we think it **could be more clear.** Tucows’ Recommended Language for Addendum I: *Note: this Addendum I applies to contracted parties providing WHOIS (available via port 43) or web-based Whois directory services only if required by the Registrar Accreditation Agreement or ICANN Consensus Policy.*” (Tucows)
<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/tucows-14-10-2022>

Background:

1. **“The document** gives the date the EPDP Team issued its Initial report and the date the GNSO Council adopted the Final Report, but **should also give the date of the Final Report (20 February 2019).” (ALAC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/policy-staff-in-support-of-the-at-large-community-at-large-advisory-committee-alac-30-11-2022>

Comments suggesting the following sections in the draft Registration Data Policy DO NOT accurately reflect the policy recommendations.

Eight groups / organizations provided comments suggesting the following areas within the drafted policy language did not accurately reflect the policy recommendations.

Section 1:

1. **“Section 1 should** be updated to **use the defined term “Processing” in Section 3.4.** The Consensus Policy is applicable to all aspects of registration data, not just processing.” **(BC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

Section 2:

1. **“The Scope** as proposed in **Section 2.2 goes beyond the purposes described in the data processing agreements since the data processing agreements do not reflect the purposes for which third parties can request the disclosure of the registration data under applicable law.** The DPAs must be written to be consistent with the Consensus Policy and cannot create a carve out for the community recommendations. The EPDP Phase 1 team worked hard to document and detail the data processing activities and responsible parties associated with gTLD registration data in Recommendation #20 of the Final Report. This was necessary as it formed the foundation of the rest of the recommendations agreed to by the team. If DPAs included community recommendations, any changes or deviations from the community, no matter how small or nuanced, from the agreed-to text of Recommendation #20 would undermine the current consensus policy and thus require a detailed review and impact assessment. **The BC is concerned that the (unpublished) DPA,** the work of an opaque negotiation outside of the ICANN multistakeholder process, **may in fact result in a situation where the GNSO and Board approved Phase 1 consensus policy would become irrelevant.** This limitation contradicts the policy as recommended by the EPDP since it does not address recommendation 1, (including Purpose 2 regarding third party purposes). **As a result, Section 2.2 should be deleted, or include a reference to these purposes.** One additional concern: because Data Processing Agreements (DPAs) are not yet negotiated, it is difficult to determine what the "purposes

identified in the Data Processing Agreement" are. Further, implementation note A provides for transfer of data that may be outside the scope of this policy. Without knowing what the DPA will specifically contain, it is difficult to comment on the impact of Note A. In addition, DPAs may be renegotiated by the parties. As a result, it is necessary to establish a process for community comment on any changes." (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

2. **"Section 2.2 is incorrect and inappropriate as drafted.** This policy's scope is not limited to only the purposes listed in yet to be created Data Protection Agreements "DPA" (and assuming agreements are in place, they would be subject to change over time). The **scope of this policy clearly includes the following** processing, notwithstanding the existence of further Data Protection Agreements: **collection; processing; publication; and, importantly, disclosure to third parties as required by this policy and/or governing law.** The **absence of required DPAs has put numerous initiatives at ICANN in limbo.** This certainly true for any type of program that contemplates data management and access. The **IPC reiterates the urgency of ICANN completing negotiations with the Contracted Parties to facilitate data processing and data access to the benefit of the entire multistakeholder community.**" (IPC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/ipc-05-12-2022>

Section 3:

1. **"Delete 3.9, or specifically call out the definitions in those agreements since there may be contradictions or unintended consequences.** For example, the terms "natural person" and "legal person" are not defined. While these terms often have standard meanings in a country's laws, those standard meanings differ from country to country. **To facilitate better compliance with privacy regulations in the future, these terms should be defined.** Definition of "Urgent Requests" is too narrow and **should include "imminent or ongoing serious cybersecurity incidents"** (such as those deriving from large scale ransomware, malware or botnet campaigns, which may for example affect consumer protection and would require an immediate need for disclosure) **regardless of whether the target is critical infrastructure."** (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>
2. **"Point 3.8 under Definitions has a grammatical/semantic error, implying that there could be such a thing as "a threat TO serious bodily injury" or "a threat TO child exploitation".** The clause "...an imminent threat to life, serious bodily injury, critical infrastructure, or child exploitation..." should contain the correct preposition for each enumerated item related to the word "threat". **The corrected clause will then read as follows: "...an imminent threat to life, of serious bodily injury, to critical infrastructure or of child exploitation..."**" (CORE Association)

<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/staub-werner-21-11-2022>

3. **“Section 3.10 appears to be inconsistent with contract drafting principles and should be deleted in favor of explicit language** being used throughout where necessary. This is a matter of good business practice and should be employed to avoid the current confusion that exists with ICANN contracts with vague or imprecise language.” (IPC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/ipc-05-12-2022>
4. **“The GAC acknowledges the role of the GDPR in serving as a catalyst for this policy and notes that the precise wording of these definitions has no bearing on parties’ obligations to comply with applicable law.** Nevertheless, the **GAC recommends that in some circumstances greater specificity could be useful, including on “consent”** (the GDPR requires the provision of consent for each purpose.) and **“personal data,” which would benefit from greater clarity around the meaning of an identifiable natural person.** Further, the GAC recommends the addition of text **making clear that no costs will be borne by those willing to access “published” data.** Finally, while the GAC is cognizant of maintaining a narrowly tailored set of circumstances warranting “urgent requests for lawful disclosure,” to ensure contracted parties are able to respond efficiently to these requests, the **GAC recommends that this category of urgent requests include “imminent or ongoing serious cybersecurity incidents”** (such as those deriving from large scale ransomware, malware or botnet campaigns, which may for example affect consumer protection and would require an immediate need for disclosure) **regardless of whether the target is critical infrastructure.”** (GAC) <https://gac.icann.org/statement/public/gac-comments-registration-data-consensus-policy-21nov22.pdf>

Section 4:

1. **“The EPDP Final Report called for implementation of the recommendations one year from the Report (which was published in 2019 (almost three years ago). There is no reason that the EPDP’s recommended proposed timeline for implementation should be ignored. By the time the final policy documents are approved and the 18 month period begins to run, it will likely be implemented in late 2024, which will be over 5 years from the Final Report, which is highly problematic for an expedited policy process.”** (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>
2. **“The EPDP Recommendations were issued in February 2019 and expected to be approved by the GNSO and Board in short order. The EPDP team (including representatives of contracted parties) understood that it would take some time to translate the recommendations into policy and then to have contracted parties implement that policy. Accordingly, Recommendation 28 extended the validity of**

terms within the Temporary Specification to allow for the creation and implementation of the policy. After due consideration the EPDP team set a deadline for contracted party compliance at 29 February 2020 (1 year after issuance of the Phase 1 report). Clearly the EPDP team underestimated the amount of time needed to translate the recommendations into policy. However, the EPDP team, including registry and registrar representatives unanimously believed that the allowed period was sufficient for contracted party implementation. Given Recommendation 28, and the fact that these recommendations are reasonably consistent with the Temporary Specification, and that the differences have been well known now for several years, the ALAC believes that allowing an additional 18 months for contracted party implementation is excessive and uncalled for.” (ALAC)

<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/policy-staff-in-support-of-the-at-large-community-at-large-advisory-committee-alac-30-11-2022>

Section 5:

1. “The second paragraph of section 5 should be updated to be treated the same as the Registrar agreements since the EPDP Phase 1 Policy did not update or eliminate the Thick WHOIS policy. As a result, all registries would need to have DPAs in place. In adopting the EPDP Phase 1 Recommendations, the Board resolution on May 19 confirmed the thick whois policy and specifically called for the EPDP Phase 2 Report to determine whether thick whois policy was to be altered. See the Scorecard for Recommendation 27: Adopt Recommendation. *“Phase 2 should examine and transparently report on whether these Recommendations require modification of existing Consensus Policies including, specifically, the Thick WHOIS Transition Policy.”* Since the Phase 2 Report did not identify thick whois as one that required modification, the Thick WHOIS policy cannot be eliminated through the IRT’s work.

Moreover, the implementation plan is not consistent with the GNSO’s subsequent resolution with regard to the thick WHOIS policy. On Jan 21, 2020, the GNSO attempted to reconcile the thick whois policy with the EPDP Phase Recommendation. In doing so, it resolved that: The GNSO Council determines that the *Recommendation #7 language, “must be transferred from registrar to registry provided an appropriate legal basis exists and data processing agreement is in place” should be included in the Registration Data Policy in order to conform with the intent of the EPDP Phase 1 Team’s policy recommendation and the subsequent GNSO Council adoption* (“GNSO Council Input”). This did not overrule thick whois but it instead confirmed its existence and required a data processing agreement to be in place with the registries. This reading is consistent with Recommendation 19, where it states that: The EPDP Team recommends that ICANN Org negotiates and enters into required data protection agreements, as appropriate, with the Contracted Parties. And Recommendation 20 where it recognizes that there is a registrar and registry purpose to access personal data: To establish the rights of a Registered Name Holder in a

Registered Name; to ensure that a Registered Name Holder may exercise its rights in the use and disposition of the Registered Name Recommendation 20 then identifies the legal basis for registries and registrars to process the personal data as 6(1)(f) or 6(1)(b).

Since NIS2 has been adopted (following the EU parliament vote on 10 Nov and Council's vote on 28 Nov), **there is an additional legal basis applicable** (Compliance with law), so **the implementation of thick whois is consistent with EU law**. Specifically, Recital 109 of NIS2 states that: ***“For that specific purpose, TLD name registries and entities providing domain name registration services should be required to process certain data necessary to achieve that purpose. Such processing should constitute a legal obligation within the meaning of Article 6(1), point (c), of Regulation (EU) 2016/679.”*** As a result, **Section 5 must not divert from the EPDP's language and require DPAs for all registries**. As a result, **the new IRT proposed text** needs to be stricken because it **is inconsistent with the Final Report: STRIKE** “Where such agreements between Registry Operator or Registrar and ICANN are required to comply with applicable law“ **STRIKE** "upon request" from "ICANN MUST upon request and without undue" **STRIKE** "If Registry Operator or Registrar determines that such agreements are required by applicable law, Registry Operator and Registrar MUST make the request without undue delay pursuant to this policy.

In any event, it's important to note that **DPAs are not required to transfer data that is not covered by GDPR - such as the data of legal persons**. As a result, **transfer of non-personal data as required by the EPDP policy needs to be implemented**. Because DPAs are not yet negotiated, it is difficult to comment with specificity. Further, **the DPAs may be renegotiated at a later time, based on one party's determination that applicable law now requires changes to the DPA**. Because these DPAs form a **critical element of the implementation and understanding of this policy, there should be some opportunity for community comment and input on these changes**.

Finally **this paragraph** needs to be modified, since it **creates a loophole that can go beyond what is necessary to comply with applicable law**: The data protection agreements MAY also be modified and updated from time-to-time as necessary to comply with applicable law based on additional guidance from relevant data protection authorities as provided for by applicable law. Finally, it's important to note that DPAs are not required to transfer data that is not covered by GDPR - such as the data of legal persons. As a result, that portion of the policy needs to be implemented.” **(BC)**
<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

2. "We strongly urge **ICANN to collaboratively finalize and then sign the DPA which has been in discussion for several years**. The language in the Draft Registration Data Consensus Policy is **ambiguous where the Recommendations of the EPDP Phase 1 are not**. For example, the Draft Registration Data Consensus Policy says **“relevant third party providers”** but does not indicate who can designate third party providers as **“relevant”**. The EPDP Phase 1 Recommendations clearly intended

Contracted Parties to be able to designate third party providers, both to themselves and to ICANN, as “relevant”. Further, **ICANN MUST enter into data protection agreements with Data Escrow Providers** but the language in the Draft Registration Data Consensus Policy allows ICANN to avoid this requirement because of its linguistic ambiguity. **Tucows’ Recommended Language for Section 5: *If Registry Operator or Registrar determines that such agreements are required by applicable law, Registry Operator and Registrar MUST make the request without undue delay pursuant to this policy for data protection agreements between the Contracted Party and ICANN and for data protection agreements between ICANN and a relevant third party provider. ICANN MUST without undue delay enter into data protection agreement or agreements upon such request.***” (Tucows) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/tucows-14-10-2022>

3. **“The first paragraph does not need to be policy language, but it does need to be acted upon.** It is unacceptable to implement this policy without first having these critical agreements in place. **The intent and the language of the policy recommendations require agreements at the outset; postponing the implementation of agreements contravenes the policy. Such an outcome is contrary to intent and the language of the policy recommendation, and should not be supported by the community, and is not supported by the IPC.** The second and third paragraphs are absolute misinterpretations of the policy. **The relevant recommendation is meant to be binding on ICANN to enter into the agreements, and is not meant to create an obligation for a Contracted Party to take this up with ICANN.** This was clearly the intent of the EPDP team, as evidenced by the plain language of the policy recommendation. **The final paragraph should say “from relevant sources” (which could include e.g. courts of law), and should not be limited to “data protection authorities” which are uniquely European and which most likely does not include all relevant authorities.”** (IPC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/ipc-05-12-2022>

Section 6:

1. **“In 6.1, Registrars should not have an option to exclude the Organization Field when collecting registrant data,** since it is a mandatory field for any registrant that is an organization. As a result, **6.1 needs to be updated to require Organization after the Name Field.** In 6.1, **Registrars should not have an option to exclude Technical Fields,** since it is a mandatory field if the registrant elects to provide it. As a result, **6.1 must be updated to require these fields as reflected in the table in the Phase 1 Final Report.** The **Reseller Field also is required to be listed in the fields collected by the Registrar in 6.1,** as was clear in the EPDP Phase 1 Final Report. Reseller can be left blank if the Registrar does not use resellers. But reseller data needs to be processed if the data is provided, per the Final report in the footnote where it says “In both cases, if data is provided, it must be processed.” (Footnote 7 on page 7 of the final report) **The WHOIS Server field is also required and was not a drafting error as**

suggested by the Report: “Registrar Whois Server” value is only required to be generated if required by the Registrar Accreditation Agreement or ICANN Consensus Policy. (See “Drafting Error” 2)” **This element needs to be preserved.** As a result, **the last sentence of 6.1 must be deleted.** Indeed the sentence is inconsistent since it states that “Registrar Whois Server” value is only required to be generated if required by the Registrar Accreditation Agreement or ICANN Consensus Policy. (See “Drafting Error” 2).” Since the EPDP Phase 1 Final Report IS creating a consensus policy, it’s obvious that **the Registrar WHOIS Server IS now a requirement going forward since the Final Report correctly lists the Registrar WHOIS Server as a requirement in the table for Recommendation 5.**

Regarding the **deletion of the Administrative Contact**, we note that **implementing this change will violate the newly adopted NIS2 language which requires the collection of specific data** in Article 28, Section 2 including: **“the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.”** As a result, **the Consensus Policy should also require the collection, transfer and disclosure of the Administrative Contacts.”** (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/ipc-05-12-2022>

2. “The “are to” language in **Recommendation 5 does not use MUST language**, so there is no binding policy language and **6.3 should be MAY.”** (IPC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/ipc-05-12-2022>

Section 7:

1. “The **Reseller Field MUST be transferred if data resides in the field.** Reseller can be left blank if the Registrar does not use resellers. But **reseller data needs to be processed if it exists**, per the Final report in the footnote where it says **“In both cases, if data is provided, it must be processed.”** (Footnote 7 on page 7 of the final report)” (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>
2. **“7.3 neither captures the intent of EPDP Phase 1 nor is it compatible with Thick WHOIS policy**, nor is it appropriate policy language. Again, it is inappropriate for this policy to contemplate that data processing agreements may not be in place, because the policy recommendations and this policy itself requires such agreements. Moreover, whether a legal basis exists is and will be a matter of fact, not of opinion. Even if it were a matter of opinion, it is ICANN’s opinion as the enforcer of this policy and the Thick WHOIS policy which must control, not the CP’s opinion. **Recommendation 7 did not contemplate that CPs would be able to eliminate the Thick WHOIS policy merely by deciding by themselves that “no legal basis exists.”** This intention was subsequently

confirmed by both the Board and GNSO Council. However, **the language as drafted in Implementation Note B would produce such an unacceptable result and therefore must be deleted.**” (IPC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/ipc-05-12-2022>

Section 8:

1. **“The Reseller Field MUST be escrowed if data resides in the field.** Reseller can be left blank if the Registrar does not use resellers. But **reseller data needs to be processed if it exists**, per the Final report in the footnote where it says “In both cases, if data is provided, it must be processed.” (Footnote 7 on page 7 of the final report)” **(BC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>
2. “Section 8 does not accurately reflect the intent of the Registration Data Consensus Policy. ” **(IPC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/ipc-05-12-2022>

Section 9:

1. **Section 9. Publication of Domain Name Registration Data:** “As suggested in the definition section, the **GAC recommends clarifying that publicly available means accessible free of charge the proposed change is as follows:**
 - a. 9.1.1 **“In responses to RDDS queries, Registrar and Registry Operator MUST Publish free of charge the following data elements:”**
 - b. The GAC refers to comments formulated above in relation to the collection of data as regards the distinction of legal and natural persons. With **regards to the publication requirements and for legal persons it is recommended to publish the additional data fields:**
 - i. **Name of registrant,**
 - ii. **Phone number of registrant,**
 - iii. **A generic/functional email of registrant**
 - iv. **These data should be added in the list of section 9.1.1.** Moreover, the data referred to under section 9.1.6 (and **especially registrant name, phone number and email**) **should not be redacted** in the event the registrant is a legal person.
 - c. 9.2.1 We acknowledge that **the wording on voluntary legal/natural differentiation stems from EPDP Phase 1 Recommendation 17.** However, this provision (9.2.1) **gives a lot of uncertainty as it allows each contracted party to decide whether they want to redact (all) information** based on a unilateral assessment of the existence of valid commercial or technical reasons, **making the policy volatile.** There is a **need for a more uniform application.**

-
- d. 9.2.6. **The need to distinguish between legal and natural registrations also impacts this provision.**
- “9.1.7. In responses to RDDS queries, Registrar and Registry Operator MAY Publish the Reseller data element.”* As described in the GAC feedback to Section 6 above, the **GAC appreciates the step taken to clarify registrar distribution channels via inclusion of the Reseller data element**, but views this element as a necessary component for understanding the roles and responsibilities (e.g., for appropriate routing of law enforcement / court orders) to the entities best positioned to respond to them. **The GAC therefore suggests:**
- i. **9.1.7. In responses to RDDS queries, Registrar and Registry Operator SHOULD Publish the Reseller data element(s) for the Reseller with a direct relationship with the Registrant..**
- e. **Overlap of Section 9. Publication of Domain Name Registration Data & Section 10. Disclosure Requests:** “10.1. Registrar and Registry Operator MUST publish on their homepage a direct link to a page where the mechanism and process for submitting Disclosure Requests is detailed. The mechanism and process MUST specify (a) the required format and content of requests, (b) the Registrar’s or Registry Operator’s means of providing a response to the requestor, and (c) the anticipated timeline for responses.” The **GAC supports inclusion of information on registrar websites pertaining to the mechanism and process for submitting Disclosure Requests**, however, **the GAC notes that a) any requestor seeking unredacted information may not know to look there**, and b) **the requestor has already viewed** the single best channel for sharing such mechanism and process information: **the published registration data itself**. The **GAC therefore suggests** the publication of such “mechanism and process” information within the Registration Data **as follows:**
- i. **“9.1.1 In responses to RDDS queries, Registrar and Registry operator MUST Publish the following data elements:”**
 - ii. **9.1.1.12 A direct link to a page where the mechanism and process for submitting Disclosure Requests is detailed.**

Section 10:

1. **“The BC supports the GAC’s comment regarding Section 10.1** - quoted below: “The GAC supports inclusion of information on registrar websites pertaining to the mechanism and process for submitting Disclosure Requests, however, the GAC notes that a) any requestor seeking unredacted information may not know to look there, and b) the requestor has already viewed the single best channel for sharing such mechanism and process information: the published registration data itself. The GAC therefore suggests the publication of such “mechanism and process” information within the Registration Data as follows: “9.1.1 In responses to RDDS queries, Registrar and Registry operator MUST Publish the following data elements:” ... 9.1.1.12 A direct link to a page where the mechanism and process for submitting Disclosure Requests is detailed.”

Additional comment to subparagraph **10.6: urgent requests require immediate assistance**. Phishing and fraud schemes. Section 3.18.2 of the RAA states that “[w]ell-founded reports of Illegal Activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report.” Since **registrars already have staff who are able and authorized to respond to critical situations within 24 hours, this same timeline should apply to reveal requests for critical requests**. In addition, since the **recently approved EU NIS 2 Directive allows an absolute maximum of 72 hours for response to ALL requests for access (not just critical requests), the policy should conform to this new requirement rather than have contracted parties adopt a standard that will not satisfy these new requirements.)** (BC)
<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

2. **“Paragraph 10.6 regarding Urgent Requests for Disclosure misapplies the approved Phase 1 policy recommendations by failing to implement expedited timeframes consistent with the nature of responding to emergency requests for disclosure.** For context, EPDP Recommendation 18 stated that: *A separate timeline of [less than X business days] will [be] considered for the response to ‘Urgent’ Reasonable Disclosure Requests, those Requests for which evidence is supplied to show an immediate need for disclosure [time frame to be finalized and criteria set for Urgent requests during implementation]. [Emphasis added].*

Notably, the Phase 1 Recommendations highlighted that these urgent requests relate to “an immediate need for disclosure.” The implementation team defined urgent requests (Definition 3.8) in a manner consistent with such an immediate need: *“Urgent Requests for Lawful Disclosure” are limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure, or child exploitation in cases where disclosure of the data is necessary in combatting or addressing this threat. Critical infrastructure means the physical and cybersystems that are vital in that their incapacity or destruction would have a debilitating impact on economic security or public safety.*

As stressed in the section pertaining to definition, **the GAC recommends to include in the scope of urgent requests other circumstances generating an immediate need for disclosure and which would otherwise be included in the regular requests** (maximum response time of 30 days), **in particular significant cybersecurity threats or incidents** (such as those deriving from large scale ransomware, malware or botnet campaigns) **regardless of whether the target is critical infrastructure**. Furthermore, in relation to the timeline, the GAC notes that despite the immediate need for such information, the implementation team construed the Phase 1 recommendations to permit a two business-day response period followed by one business-day extension under certain circumstances. Put simply, **three business days (which could stretch to seven calendar days depending on weekends and intervening holidays) is not a reasonable time period for responding to urgent requests**. This is especially true

because “urgent” requests apply only to emergency situations involving imminent threats to life and critical infrastructure among other things.

The implementation team misinterpreted the Phase 1 recommendations by applying the same two business-day acknowledgment period for general requests to urgent requests. This flawed interpretation had the effect of prolonging the timeframe to respond to an urgent request. However, the foundational logic of dealing with “urgent” requests separately was to streamline the entire process because these requests deal with time-sensitive matters that involve threats to life, safety, or vital infrastructure. Hence, it would be neither reasonable nor logical to view the 2-day acknowledgement provision as overriding or extending the separate timeline for responding to urgent requests. More specifically, the acknowledgement time for general requests should not delay the contemplated expedited timeline for urgent requests. The GAC believes that this interpretation conflicts with the clear Phase 1 directive to develop “a separate timeline” for the response to urgent requests. **The GAC recommends that the implementation team must revisit this issue to ensure that responses to urgent requests are in fact expedited in a manner consistent with an emergency response.”(GAC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/governmental-advisory-committee-21-11-2022>

3. “The Final Report said, “A separate timeline of [less than X business days] will be considered for the response to ‘Urgent’ Reasonable Disclosure Requests, those Requests for which evidence is supplied to show an immediate need for disclosure [time frame to be finalized and criteria set for Urgent requests during implementation].” It is important to note the definition of “URGENT” requests. “Urgent Requests for Lawful Disclosure” are limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure, or child exploitation in cases where disclosure of the data is necessary in combatting or addressing this threat. Critical infrastructure means the physical and cyber systems that are vital in that their incapacity or destruction would have a debilitating impact on economic security or public safety. It is unfortunate that the report specified “business days” as the basis for the policy. That being said, **to set it at TWO days in light of the definition of Urgent requests is totally unreasonable! It is not uncommon to have three consecutive non-business days resulting in a potential of 5 calendar days for responses to URGENT requests.** The ALAC notes that the RAA already includes **provision 3.18.2: Well-founded reports of Illegal Activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report. As such, registrars must already have staff who are able and authorized to respond to critical situation within 24 hours.** There is no reason not to use these same capabilities for situations where there is imminent threat to life, serious bodily injury, critical infrastructure, or child exploitation. The ALAC also notes that **the recently approved EU NIS 2 Directive allows an absolute maximum of 72 hours for response to ALL requests for access (not just critical**

requests).”(ALAC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/policy-staff-in-support-of-the-at-large-community-at-large-advisory-committee-alac-30-11-2022>

4. “**Sections 10.5 and 10.6 of the Draft Policy** propose deadlines for Registrars and Registry Operators for acknowledging receipt of Requests for Lawful Disclosure. **INTA believes that these turnaround times are unduly and unnecessarily long.** The responses will undoubtedly be generated by an automated system, rather than by an individual looking through the contents of a file cabinet. Specifically, **the draft proposes that a Request for Lawful Disclosure shall be acknowledged without undue delay, which may be as much as two business days from receipt.** Both businesses and government agencies routinely generate acknowledgement of a submission virtually instantaneously. It is **difficult to imagine any reason why it could or should take two business days to generate an automated response.** Of greater concern, the **draft proposes** that a Registrar or Registry Operator may take as long as **thirty calendar days to respond to a Request for Lawful Disclosure.** If the criteria for providing access to non-public Registration Data are reasonable and clearly defined, **thirty calendar days for a response is unnecessary and wholly too long.** Section 10.2.3 proposes that a Reasonable Request for Lawful Disclosure must provide information about its legal rights and the basis for its request.

The draft, however, does not provide any indication as to the circumstances under which a request will be evaluated other than to say that it must be considered on its merits. The only guidance as to whether a request should be granted appears in Section 10.7.2, which states that if the request for data is refused, the Registry Operator or Registrar must provide an analysis and explanation of how the fundamental rights and freedoms of the data subject were weighed against the legitimate interest of the request. It should be made clear that Registrars and Registry Operators are not to decide whether the requesting party will be entitled to relief on the merits of its claim, just whether they have set forth a reasonable basis for a potential claim where the requested information should be provided so the claim may move forward. Moreover, without further guidance as to whether a request should be granted, each Registrar and Registry Operator would be free to apply its own subjective criteria in determining whether a request for data is reasonable and how to balance the rights and interests of the data subject and the requestor, which will undoubtedly lead to inconsistent results, which should not be allowed. INTA agrees that protecting the right to privacy is of great importance. Even so, **it must be recognized that there are occasions where other interests, such as the harm incurred by end users may outweigh the right to privacy.**”(INTA) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/constituency-intellectual-property-05-12-2022>

Section 11:

-
1. **“11.1.2 should be MUST maintain log files to confirm relay of communications from requestor to tech email address.** Rec #13 explicitly says “and which shall contain confirmation that a relay of the communication between the requestor and the Registered Name Holder has occurred” Additionally, all of the **log file requirements should be amended to allow logging of information that is not Personal Information.” (BC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>
 2. **“As drafted, 11.1.1 and 11.1.2 are impossible for CPs to comply with in modern logging software.** The **redactions/removals called for** are overly burdensome in their redaction requirements to the point where they actually **conflict with the rest of the good logging requirements in Section 11.** It is almost understandable if contents must not be logged, but a **log that does not contain the sender or recipient would be useless to the community.” (IPC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/ipc-05-12-2022>

Section 12:

1. **“Section 12 only sets a minimum retention period of no less than fifteen (15) months. The Provision should be further reviewed considering article 5 of the GDPR and data minimization principles”(AFNIC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/afnic-21-11-2022>
2. **“Registrar MUST retain those data elements necessary for the purposes of the Transfer Dispute Resolution Policy for a period of no less than fifteen (15) months following end of Registrar’s sponsorship of the registration or an inter-registrant (change of registrant) transfer of the registration.” The GAC recommends reviewing this provision, which only sets a minimum (mandatory) retention period, whereas the requirement under the GDPR is to limit retention to the period necessary to fulfill the purpose of processing.“(GAC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/governmental-advisory-committee-21-11-2022>

Addendum II:

1. **“This should be clarified to require that the RNH field have an accurate value before deleting the Organization Field** provided by the registrant. Rec #12 says, “If the registrant declines, or does not respond to the query, the Registrar may redact the Organization field, or delete the field contents. If necessary, the registration will be reassigned to the Registered Name Holder.” Implementation says, “Prior to deleting Registrant Organization value, Registrar MUST ensure that the value for the required Registered Name Holder Data element in Section 6.1.9 has been collected.” **(BC)**

<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

Implementation Notes:

1. “This **implementation should be paused to take into account the approved EU NIS2 Directive** (Nov-2022) and the required transposition by EU member states. **Specifically: Publication requirements, specifically for legal persons Accuracy and proactive verification requirements for registrant data Legal basis for processing, transfer from registrar to registry, and disclosure requirements, with standards for response and service level**” (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>
2. “As noted above, **Implementation Note B.3 and B.4 are inappropriate and unacceptable.**” (IPC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/ipc-05-12-2022>

Background:

1. “**Background does not reflect important considerations for the work of the EPDP: Original mandate from the Board for developing policy that “preserves Whois to the greatest extent possible while complying with GDPR”** check and cite. **Background should document that the WG was asked to develop policy that could evolve with changes in GDPR interpretation by courts and member states, and the majority rejected that request. With the NIS2 adopted in Nov-2022, it is now clear that evolution should be part of the implemented policies. Background should explain specifically how EPDP recommendations could possibly lead to making it optional for registries and registrars to maintain Thick Whois consensus policy. Specifically, the background should document Thick Whois changes after the policy was adopted by the board (Scorecard).**” (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

Comments suggesting Additional Concerns or Issues with the following sections in the draft Registration Data Policy

Seven groups / organizations provided comments noting additional concerns or issues were identified in the following sections of the draft policy.

Section 1:

1. One commenter noted that section 1 of the draft Registration data policy required further clarification but did not expand on the type of clarification required. (CORE Association)

<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/staub-werner-21-11-2022>

Section 2:

1. “The GAC notes that **Section 2.2** of the Draft Policy stipulates that “Registrar Operator’s and Registrar’s Processing of Personal Data contained in Registration Data for purposes other than the purposes identified in the Data Protection Agreement required by Section 5 is beyond the scope of this Policy”. **The GAC recommends clarifying this language as it is unclear what “other purposes” includes.** This is especially relevant given that **Data Protection Agreements in Section 5 are made conditional on an assessment by contracted parties and the lack of a common model for data processing agreements makes it unclear what purposes could be covered therein.**” (GAC) <https://gac.icann.org/statement/public/gac-comments-registration-data-consensus-policy-21nov22.pdf>
2. “**The expression “other purposes” should be further clarified to identify what purposes would be covered under section 2.2”** (AFNIC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/afnic-21-11-2022>
3. “**Section 2.2 is incorrect as drafted. This policy’s scope is not limited to only the purposes listed in Data Protection Agreements “DPA” that are under discussion.** Even when negotiated and agreed upon, those agreements are subject to change as conditions change. **The scope of this policy clearly includes data collection, processing, publication, and, importantly, disclosure to third parties as required by this policy and/or governing law. The absence of required DPAs has put numerous ICANN initiatives on hold.** Data Accuracy Scoping is a good example of where the absence of a DPA has stalled critical portions of the work. **INTA notes the urgency for ICANN to complete negotiations with the Contracted Parties for appropriate DPAs. The negotiations should be prioritized and expedited to facilitate data processing and data access to the benefit of the community.**” (INTA) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/constituency-intellectual-property-05-12-2022>

Section 5:

1. “**Section 5** stipulates that “Data Protection Agreement ICANN, gTLD Registry Operators, and accredited Registrars **MUST** enter into required data protection agreements with each other and with relevant third party providers contemplated under this Policy where applicable law requires.” **The GAC recommends review of this provision to clarify the obligation for the cited parties to enter into a data protection agreement.** First, if there are legal requirements, then the relevant laws establish the obligation regardless of these policies. Second, **the policy implementation** appears to be internally inconsistent because it both obliges the parties to enter into DPAs but then qualifies this obligation by indicating that it is subject to any

'applicable law.' This makes it unclear whether there is truly an obligation or not. Moreover, it is unclear how operators would assess which laws establish such a requirement. This risks making uniform implementation inside the same gTLD difficult. The GAC would support making the Data Processing Agreement unequivocally mandatory by deleting the reference "where applicable law requires." The GAC notes the importance of clearly defined roles and responsibilities for the processing of the data in the Registrar Agreements. This is also supported by the current temporary specifications, which include the following provision: "Registry Operator *MUST* include Processing provisions in its Registry-Registrar Agreement with Registrar concerning the handling of Personal Data in a manner that complies with applicable requirements of Article 28 of the GDPR" (GAC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/governmental-advisory-committee-21-11-2022>

Section 6:

1. **"6.3. The GAC finds this section unclear as it could imply that under certain circumstances the contact details of the technical contact may replace the contact details of the registrant. The present data policy should ensure that the contact details of both the registrant and the technical contact are collected.**

"6.4 Registrar MAY generate the Reseller data element value.

- a. **The GAC observes that the domain name industry has evolved considerably since ICANN's inception, and today includes roles and entities which may not have existed in previous RDDS systems; similarly, new entities may be created tomorrow which have yet to be conceived of today. In recognition of this, the GAC supports the inclusion of corporate entities inherent to the registrar's distribution channel (such as the RDAP Response Profile entity 2.5 enumerating the "reseller" role) as it is the purpose of the RDDS system to enumerate roles and responsibilities relevant to domain name registrations; such entities should be included in an RDAP response, when they exist. This would also prove as a benefit in highlighting the best point of contact to deal with notifications of abuse or compromise to the party with the ability to act the quickest or most appropriately. To that end, the GAC suggests the following text:**

6.4 Registrar SHOULD generate the Reseller data element value, for the Reseller with a direct relationship with the Registrant. Further, the GAC views the current definition of "Reseller" within the 2013 Registrar Accreditation Agreement (RAA)² as potentially inclusive of privacy and/or proxy services offered by entities within the registrar's distribution channel. **The GAC seeks clarification as to which entities SHOULD or SHOULD NOT be considered "Resellers" within the Consensus Policy;** to the extent entities exist within the registrar distribution channels which were assumed by the authors of the Consensus Policy to not fall within the Reseller data element, the GAC would

appreciate explicit clarification. In such cases, **the GAC would benefit from further clarification as to which data elements SHOULD be used for each category of entities existing in registrar distribution channels. If data elements do not currently exist for such entities, the GAC would view it as constructive to create and incorporate within the Consensus Policy such elements.**

6.5 – 6.6: “If provided by the Registered Name Holder, Registrar MUST collect the following data element values”. The GAC acknowledges that this wording stems from Recommendation 12 of EPDP Phase 1, however **the GAC reiterates that these data elements may change as a result of pending policy recommendations, particularly the approved Phase 2A recommendations. EPDP Phase 2A has required the functionality of distinguishing between legal and natural persons and the GAC believes that such distinction has not been taken into account in the present Draft Policy. In particular, data such as ‘the registrant organisation’, though not essential for registrants who are natural persons, should nevertheless be collected when the registrant is a legal person. This information can thus be optional for natural persons but should be mandatory for legal persons. As the GAC has stressed on multiple occasions, personal data protection regulations, including the GDPR, apply to the processing of personal data of natural persons and not legal persons. Therefore, the contracted parties should collect and make data of legal persons publicly available. Additional safeguards may be considered for the case where the email address of a legal person contains personal data, in which case a functional email address can be published instead.”(GAC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/governmental-advisory-committee-21-11-2022>**

Section 7:

1. “7.3. “Registrar MUST transfer the following data elements to Registry Operator provided an appropriate legal basis exists and data processing agreement is in place.” As already stressed in previous sections, **the lack of clarity regarding the obligation to have a Data Processing Agreement does not help implementation and enforcement of this policy. The GAC recommends that the data policy be clear as regards the obligation of data protection agreements and that it includes appropriate data protection safeguards, including for the cases of transfers. 7.4. The GAC reiterates the importance of distinguishing between legal and natural persons (see above).”(GAC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/governmental-advisory-committee-21-11-2022>**

Section 9:

-
2. **“Paragraph 9.2.1 allows the redaction of non Personal Data contained in the Registration Data if there is a "commercially reasonable," purpose to do so.** The fundamental purpose of the specification is to facilitate compliance with applicable privacy law. Whether redaction of non-personal data impacts a Registry Operator or Registrar's commercial business is beyond the scope of the process. More to the point, **the use of the broad term "commercially reasonable" without definition undermines the fundamental purpose of a specification by inserting significant ambiguity into the specification.** Furthermore, **the proposed implementation is not consistent with the new requirements of NIS2 and must be updated to ensure that all non-personal data be published free of charge.** Specifically, Recital 112 states: **“Member States should ensure that all types of access to personal and non-personal domain name registration data are free of charge.”**“ There is no reason that implementation of the NIS2 publication requirements can't be included in the consensus policy at this time, especially since it **would not be “commercially reasonable” to violate NIS2,** and because “technical feasibility” cannot excuse compliance with NIS2. Article 28 Section 4 states that: “Member States shall require the TLD name registries and the entities providing domain name registration services to make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data. **“ The implementation of the Consensus Policy should accommodate the new requirements rather than incorporate terms (such as the illegal redaction of legal person’s data), that will cause the Consensus Policy to be out of compliance with NIS2.”** (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>
3. “9.1.7 Reseller MUST be published if present/provided. 9.1.10 These MUST be published if present/provided. **The first MUST in 9.2.1 should be MAY - ICANN is in the business of enforcing policy requirements, not in the business of enforcing laws. In the fourth line of 9.2.1, the word MAY conflicts with the word “requirements.” A different word should be used (“options”?) since ICANN clearly does not intend these to be requirements. The 9.2.1(i) and (ii) carve outs are unacceptable. Each of (i) and (ii) would render this portion of the policy unenforceable as they would permit contracted parties sole discretion to do as they please.** Such an outcome would be unacceptable. **9.2.4 should include the Org field in the list which registrar MUST provide the opportunity for the RNH to consent to publication and which consent registrar MUST honor. 9.2.6 insufficiently captures this as it does not explicitly require the registrar to offer the option. In Sections 9.2.2.3 and 9.2.2.4 - Registries should be required to publish if they have the Org and City data elements.”** (IPC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/ipc-05-12-2022>

Addendum I:

-
1. **“Web-based lookups are required under the Registrar Accreditation Agreement.” (BC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>
 2. **“It seems this implicitly excludes RDAP(?), which doesn't make sense.” (IPC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/ipc-05-12-2022>

Addendum II

1. **“As noted in previous comments from many parts of the community, it would be irresponsible to allow Contracted Parties to delete Registrant Organization data.** This risks fundamentally and irreparably changing the entity responsible for domain name ownership, which is an unacceptable outcome.” (IPC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/ipc-05-12-2022>

Implementation Notes:

1. **“The final paragraph of the Draft Registration Data Policy should be completed before the Draft becomes Policy.” (Tucows)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/tucows-14-10-2022>

Comments suggesting the proposed redlines made to following redlined policies and procedures incorrectly reflect the requirements in the draft Registration Data Policy.

Three groups / organizations noted that the following proposed redlines within the policies are incorrect based on the requirements in the registration data policy.

1. Additional Whois information Policy:

- a. IPC suggested that the “redlines within the existing AWIP policy are incorrect” but did not elaborate further (IPC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/ipc-05-12-2022>

2. ERRP:

- a. **“The recommended changes include dropping the term “Registrant” and replacing with “Registered Name Holder.” This change was not part of the recommendations and this change makes the policy inconsistent with prior policies that refer to “registrant”. This policy should make clear that Registrant and "Registered Name Holder" are synonymous.” (BC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

3. **Protection of IGO and INGO Identifiers in all gTLDs Policy:**

- a. “The **recommended changes include dropping the term “Registrant” and “domain name registrant” and replacing with “Registered Name Holder.”** This change **was not part of the recommendations** and this change **makes the policy inconsistent with prior policies that refer to “registrant”**. This policy should make clear that Registrant, “Domain Name Registrant”, and “Registered Name Holder” are synonymous.”(BC)

<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

4. **CL&D Policy:**

- a. “The **requirement for maintaining a WHOIS lookup web based service on the contracted parties website’s should not be eliminated.** See the BC’s comments to the RDAP implementation posted at

<https://www.icann.org/en/public-comment/proceeding/proposed-amendments-to-the-base-gtld-ra-and-raa-to-add-rdap-contract-obligations-06-09-2022/submissions/icann-business-constituency-bc-16-11-2022>” (BC)
<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

5. **Thick Whois Transition Policy:**

- a. “The **proposed changes is to eliminate Thick Whois transition for COM, NET, and Jobs:** “As of [INSERT Registration Data Policy Effective Date] all requirements of this Policy have been superseded by the Registration Data Policy.” However, **final NIS2 text approved 10-Nov-2022 by the Parliament and approved by the Council on 28 Nov 2022 requires Thick Whois.** Specifically Article 28 states that “...member states shall require TLD name registries and entities providing domain name registration services to collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in accordance with Union data protection law as regards data which are personal data. “ **So this Policy Recommendation would require Thick Whois:** “Registry Operator and Registrar are not required to establish legal basis to process Personal Data, including transfer from Registrar to Registry Operator, if not required by applicable law” As EU member states begin transposing NIS2, **applicable law will require registrant data transfer to all registries.** So instead of eliminating the Thick WHOIS requirement, the Registry operator for COM, NET, and JOBS should propose a new transition policy, possibly drawing upon the prior transition policy and implementation plans.” (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

-
- b. **“The EPDP recommendation on the transfer of data from registrars to registries makes the implementation of the Thick Whois policy difficult, but it does not make it impossible.** This is particularly true for registrations the contain no personal information. Moreover, the **recently approved EU NIS2 requires that registries and registrars publish publicly available data, and make available redacted data to legitimate users; AND that registrars and registries cooperate so that data does not need to be collected twice.** That **implies that if registrars are the prime collector of the data** (as they are with gTLDs) **that registrars must cooperate and provide registries with the data.** **NIS 2 notes that this obligation is sufficient legal reason for processing the registration data under GDPR Article 6.1(c).** [NIS 2: Recitals 109-112 and Article 28].” (ALAC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/policy-staff-in-support-of-the-at-large-community-at-large-advisory-committee-alac-30-11-2022>

6. Transfer FOA:

- a. **“The EPDP Phase 1 Policy did not authorize these changes: - The change of “registrant” to “registered name holder.” - The deletion of “ in the event of a dispute the Registered Name Holder’s authority supersedes the administrative contact’s authority” - Footnote 1 which incorrectly attempts to define “Registered Name Holder” This definition is inconsistent with RAA Section 1.16 where it states that “Registered Name Holder” means the holder of a Registered Name. The IRT did not have authority to redefine definitions in the RAA. - Elimination of the “Transfer Contact” throughout. - Elimination of the Form of Authorization.** Indeed they create security risks since Forms of Authorizations (FOA) were intended to make transfers more secure by preventing domain name hijacking. When DPAs are implemented and more contact information is available (such as when NIS2 requirements apply to the data of legal persons and/or natural person registrants consent to the publication of their information), **the FOAs should be required rather than eliminated. - Addition of the “where required pursuant to Section I.A.2.”** throughout, such as in Section 2.2.1., 2.2.4, 4.1, 4.3 - Registrant Transfers- **Deletion of 1.1.4 in Section II.A.** Instead - **technical contact should be substituted for the administrative contact. These changes are not necessary to implement the Phase 1 Policy and should be deleted.** In addition, **more work is needed to determine whether it would be more appropriate to substitute the “technical contact” for the “administrative contact” in the transfer policy** since there may be instances where the technical contact may be more closely aligned with what was formerly the administrative contact. Indeed, this creates a security risk when there are multiple contacts (registrant and tech contact), and the registrant is unresponsive or goes out of business. Examples of where this might arise could be situations where the reseller or privacy/ proxy service is the registrant, and the technical

contact is the customer of the reseller, privacy/proxy service. This is especially important when more registrations reflect registrant information that apply to resellers or privacy/proxy providers. Instead, **the policy should replace “administrative contact” with “technical contact” to have an additional way of enabling the transfer.** (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

7. Transfer FOA Initial Authorization:

- a. **“The EPDP Phase 1 Report did not authorize these changes: - The elimination of a second form of authorization in the FOA. As a result, the policy should reflect “technical contact” in lieu of “administrative contact” throughout. - The elimination of a reference to a “WHOIS database”. The changes assume that there are no contacts in the RDS database that are public, yet ICANN policy clearly requires contacts to be published when the registrant consents, and there may be legal requirements such as NIS2 where the data of legal persons is required to be published. These changes are not necessary to implement the Phase 1 Policy and should be deleted.” (BC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

8. TDRP:

- a. **“The EPDP Phase 1 Policy did not authorize these changes: - The change of “registrant” to “registered name holder.” - Elimination of the “Transfer Contact” throughout. - Elimination of the Form of Authorization. Indeed they create security risks since Forms of Authorizations (FOA) were intended to make transfers more secure by preventing domain name hijacking. When DPAs are implemented and more contact information is available (such as when NIS2 requirements apply to the data of legal persons and/or natural person registrants consent to the publication of their information), the FOAs should be required rather than eliminated. - The deletion of a duplicate form of authorization - instead of eliminating the “administrative contact “ throughout, it should be replaced with the technical contact. These changes are not necessary to implement the Phase 1 Policy and should be deleted. See above for explanation for why these changes are inappropriate.” (BC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

9. Transfer Policy:

- a. **“The EPDP Phase 1 Policy did not authorize these changes: - The change of “registrant” to “registered name holder.” - The deletion of “ in the event of a dispute the Registered Name Holder’s authority supersedes the administrative contact’s authority” - Footnote 1 which incorrectly attempts to**

define “Registered Name Holder” This definition is inconsistent with RAA Section 1.16 where it states that "Registered Name Holder" means the holder of a Registered Name. The IRT did not have authority to redefine definitions in the RAA. - **Elimination of the “Transfer Contact” throughout.** - The requirement of a “secure method of transfer” in Section 2.2.1 before any registration data can be transferred. No secure method of transfer is needed for information that is publicly available. When DPAs are implemented and more contact information is available (such as when NIS2 requirements apply to the data of legal persons and/or natural person registrants consent to the publication of their information), this information can be shared without further restrictions as imposed by proposed implementation.

- **Elimination of the Form of Authorization.** Indeed they create security risks since Forms of Authorizations (FOA) were intended to make transfers more secure by preventing domain name hijacking. When DPAs are implemented and more contact information is available (such as when NIS2 requirements apply to the data of legal persons and/or natural person registrants consent to the publication of their information), **the FOAs should be required rather than eliminated.** - **Addition of the “where required pursuant to Section I.A.2.” throughout,** such as in Section 2.2.1., 2.2.4, 4.1, 4.3 - **Registrant Transfers- Deletion of 1.1.4 in Section II.A. Instead - technical contact should be substituted for the administrative contact.-** The language regarding “best practices” for generating AuthCodes should be strengthened to require the generation of AuthCodes, with the “best practices” to apply to how they are transmitted. These changes are not necessary to implement the Phase 1 Policy and should be deleted.

In addition, **more work is needed to determine whether it would be more appropriate to substitute the “technical contact” for the “administrative contact” in the transfer policy** since there may be instances where the technical contact may be more closely aligned with what was formerly the administrative contact. Indeed, this creates a security risk when there are multiple contacts (registrant and tech contact), and the registrant is unresponsive or goes out of business. Examples of where this might arise could be situations where the reseller or privacy/ proxy service is the registrant, and the technical contact is the customer of the reseller, privacy/proxy service. This is especially important when more registrations reflect registrant information that apply to resellers or privacy/proxy providers. Instead, **the policy should replace “administrative contact” with “technical contact” to have an additional way of enabling the transfer.”** (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

10. UDRP:

-
- a. **“The EPDP Phase 1 Report did not authorize these changes: - The elimination of a reference to a “WHOIS database”.** The changes assume that there are no contacts in the RDS database that are public, yet **ICANN policy clearly requires contacts to be published when the registrant consents**, and there may be legal requirements such as NIS2 where the data of legal persons is required to be published. - **Footnote 1 should be deleted since there is no reason to replace “WHOIS database” with Registration Data.** These **changes are not necessary** to implement the Phase 1 Policy and **should be deleted.”** (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

11. UDRP Rules:

- a. **“The EPDP Phase 1 Report did not authorize these changes: - The elimination of a reference to a “WHOIS database”.** The changes assume that there are no contacts in the RDS database that are public, yet ICANN policy clearly requires contacts to be published when the registrant consents, and there may be legal requirements such as NIS2 where the data of legal persons is required to be published. - **Footnote 1 should be deleted since there is no reason to replace “WHOIS database” with Registration Data.** - In Section 2(a)(2) - the **insertion of “Registration Data Directory Service (hereinafter “RDDS”) or in the Registration Data provided by the Registrar or Registry Operator when the Registration Data is redacted in the RDDS” is not needed.** When there is a Redacted Contact in the public RDDS queries, the unredacted RDDS would still be available to be provided under the Rules. This change implies that the Registrar can list other data (such as customer data) beyond the unredacted information - which is clearly not possible. These **changes are not necessary** to implement the Phase 1 Policy and **should be deleted.”** (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

12. URS Procedure:

- a. **“The EPDP Phase 1 Report did not authorize these changes: - In Section 4(2) - the insertion of “or to the addresses listed in the Registration Data provided by the Registrar or Registry Operator when the Registration Data is redacted in the RDDS,” is not needed.** When there is a Redacted Contact in the public RDDS queries, the unredacted RDDS would still be available to be provided under the Rules. This change implies that the Registrar can list other data (such as customer data) beyond the unredacted information - which is clearly not possible. These changes are not necessary to implement the Phase 1 Policy and should be deleted.” (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

13. URS Rules:

- a. **“Section 4 should replace the new “Registrant Data” with “RDDS”.” (BC)**
<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

14. WDRP Rules:

- a. **“The EPDP Phase 1 Policy did not authorize these changes: - The change of “registrant” to “registered name holder” throughout. - In the first paragraph the replacement of “Registration Data” is incorrect since Registration Data includes information that is not generated by the Registrant. - The deletion of the requirement to send the notice to a duplicate contact - instead of eliminating the “administrative contact “ throughout, it should be replaced with the technical contact. More work is needed to determine whether it would be more appropriate to substitute the “technical contact” for the “administrative contact” in the WHOIS Data Reminder Policy since there may be instances where the technical contact may be more closely aligned with what was formerly the administrative contact. Indeed, this creates a security risk when there are multiple contacts (registrant and tech contact), and the registrant is unresponsive or goes out of business. Examples of where this might arise could be situations where the reseller or privacy/ proxy service is the registrant, and the technical contact is the customer of the reseller, privacy/proxy service. This is especially important when more registrations reflect registrant information that apply to resellers or privacy/proxy providers. Instead, the policy should replace “administrative contact” with “technical contact” to have an additional way of ensuring that the information provided is accurate.” (BC)**
<https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

15. RDAP Technical Implementation Guide:

- a. **“As stated above the BC believes that **Web-based lookups must continue to be required under the Registrar Accreditation Agreement.** An obligation to only respond to RDAP queries using a non-human readable/parsable network protocol is insufficient to ensure Internet users have access to Registration Data as required by the ICANN bylaws.” (BC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

16. RDAP Response Profile:

- a. **“As stated above the BC believes that **Web-based lookups must continue to be required under the Registrar Accreditation Agreement.** An obligation to only respond to RDAP queries using a non-human readable/parsable network protocol is insufficient to ensure Internet users have access to Registration Data as required by the ICANN bylaws. **Attachment:** [BC Comment on Draft policy for](#)**

[gTLD Registration data.pdf \(209.17 KB\)](#) **Summary of Attachment:** The attached PDF is in lieu of completing this form, since the attachment includes formatting that should assist readers in identifying line breaks, lists, text excerpts, strike-throughs, etc. **Summary of Submission:** The final NIS2 text was adopted by the European Parliament on 10-Nov-2022. The BC and other members of the EPDP frequently cited pending NIS2 regulation in our advice to create evolution mechanisms for registrant data policy. Unfortunately, the EPDP Working Group and GNSO Council did not follow that advice. **NIS2 now requires EU Member States to enact regulation that may render some EPDP policy recommendations in conflict with law.** Specifically, **NIS2 requirements to publish registrant data for legal persons, requirements to maintain accurate registrant data, and potentially requirements for registries to maintain registrant data (i.e. Thick Whois).** The BC therefore **recommends that implementation of EPDP Phase 1 and Phase 2 be reassessed after the first EU Member State implements regulations pursuant to NIS2.** (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>

General Comments:

Below are the general comments groups / organizations provided in addition to the input above.

1. **“The i2Coalition would like to express support for the drafted Data Consensus Policy for gTLDs.** The Internet Infrastructure Coalition (i2Coalition) appreciates the opportunity to comment on Registration Data Consensus Policy for gTLDs. The i2Coalition would like to express support for the drafted Data Consensus Policy for gTLDs. This is a necessary step in properly aligning ICANN and contracted parties with the requirements of the European Union’s General Data Protection Regulation. Alongside **ICANN Org’s review of policies and procedures as per EPDP-TempSpec Phase 1 Recommendation 27, this signals important progress, in moving toward stable footing with an actual Consensus Policy.** The i2Coalition’s diverse membership represents both large and small Internet infrastructure providers such as web hosting companies, software services providers, data centers, registrars and registries. The i2Coalition has several key goals within ICANN, but chief among them is continuing to build a voice for underrepresented parts of the Internet ecosystem – in particular web hosts, data centers and cloud infrastructure providers – and ensuring that accountability and transparency are paramount. The i2Coalition brings unique representation to ICANN as it is made up of companies representing the broad ecosystem of Internet infrastructure companies.” **(Internet Infrastructure Coalition i2C)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/i2c-internet-infrastructure-coalition-18-11-2022>
2. **“The Registries Stakeholder Group (RySG) appreciates the opportunity to comment on the Draft Registration Data Consensus Policy for gTLDs.** The RySG has noted a

few areas where we believe slight changes will provide beneficial clarity for those implementing the policy but overall, the RySG is supportive of the policy. Further, the **RySG did not specifically weigh in on each impacted policy in Part II of this comment as several are specific to individual operators, but are generally supportive of the work.** The RySG appreciates the time and effort put forth by every participant across the community to craft this draft policy. **We believe it provides an important baseline for registration data processing that will provide Registry Operators certainty and flexibility.**” (RySG) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/rysg-registries-stakeholder-group-21-11-2022>

3. **“Tucows thanks the IPT and IRT for their many hours of work and diligent efforts in translating the Working Group Recommendations into Policy. The Registration Data Policy for the most part accurately reflects the Recommendations; Tucows has suggested modifications to Sections 5, and 10, Addendum I, and the Implementation Notes.”** (Tucows) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/tucows-14-10-2022>
4. **“The IPC appreciates the opportunity to comment on this draft policy, and we thank ICANN staff and the IPT for its herculean effort. Among the concerns listed above, a primary concern for the IPC is that - as required by the EPDP policy recommendations - ICANN must enter into DPAs with Contracted Parties before it can implement this policy, not after. ICANN must also ensure that this policy does not have the effect of overriding the important Thick WHOIS policy, which will be aided by the timely execution of DPAs. Specifically, ICANN must amend this draft policy to be clear that ICANN has the authority to determine whether a legal basis exists for processing WHOIS data. Failure to correct this language would result in the unacceptable outcome of Contracted Parties having sole discretion to determine at their convenience whether to comply with the Thick WHOIS policy, an outcome which would contravene the Board and community’s stated intent that this policy not supersede or undo Thick WHOIS.”** (IPC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/ipc-05-12-2022>
5. **“The Registrar Stakeholder Group (RrSG) is pleased to comment on the Registration Data Consensus Policy for gTLDs and thanks the IRT team for their efforts. In general, it is the RrSG’s position that the policies accurately reflects the policy recommendations, with some suggested clarifications. The RrSG also notes that the questions in regards to transfers are under review by the PDP Transfer Policy Review PDP.”** (RrSG) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/rrsg-21-11-2022>
6. **“AFNIC appreciates the opportunity to provide comments and inputs on the Registration Data Consensus Policy for gTLDs. We also would like to convey our thanks to the working group, the community as well as the Implementation Review**

Team (IRT) and Implementation Project Team (IPT) for the work done one. The draft Registration Data Policy mostly reflects the recommendations with regards to the collection, transfer, and publication of gTLD registration data but further clarification and slight modifications are needed to allow for a clear and consistent implementation of the policy” (AFNIC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/afnic-21-11-2022>

7. **“Newfold Digital, Inc. thanks all current and past members of the IPT and IRT for their work. We believe the Registration Data Policy presented accurately reflects the recommendations but wish for the data processing agreements, recommended to be in place between ICANN and Contracted Parties per the EPDP Phase 1 Final Report, are completed at the earliest.” (Newfold Digital) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/newfold-digital-inc-28-11-2022>**
8. **“Regarding sections 6 and 7, there has been a lot of progress in governance and community institutions outside of ICANN multistakeholder process. These important achievements should not be locked out of ICANN’s policies. Public identifiers are ways to improving the accountability of businesses while protecting the data of natural persons whose names should not be stored in corporate domain registration data. Even in the absence of a dedicated field for supplying a public identifier, the registrants should be allowed to append a URI with their public identifier in the Registrant Organization field.** Public identifiers that are appropriate to identify corporate domain holders include among others:
 - a. (1) the Legal Entity Identifier (LEI). This is a process administered by <https://gleif.org> based on ISO 17442. See https://en.wikipedia.org/wiki/Legal_Entity_Identifier
 - b. (2) Global Location Number (GLN). This is a process administered by <https://sg1.org> based on ISO/IEC_6523. See https://en.wikipedia.org/wiki/Global_Location_Number
 - c. (3) SWIFT Business Identifier Code (BIC). This is a process administered by <https://www.swift.com> based on ISO_9362. See https://en.wikipedia.org/wiki/ISO_9362.
 - d. (4) Decentralized Identifiers as described in the July 2022 W3C Recommendation <https://www.w3.org/TR/did-core/>
 - e. A minor suggestion for section 3 deals with a key clause that grammatically signifies the opposite of what is the intent; it can be corrected by adding the correct prepositions “to” or “of” for each of the enumerated items referred to by the word “threat”.” (Core Association) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/staub-werner-21-11-2022>

-
9. “The At-Large Advisory Committee (**ALAC**) has comments and concerns in regards to the following sections of this Public Comment proceeding:
 - a. **(1) Section 4: Effective Date**
 - b. **(2) Section 10: Disclosure requests**
 - c. **(3) Background Section of the Registration Data Consensus Policy**
 - d. **(4) Thick Whois Transition Policy” (ALAC)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/policy-staff-in-support-of-the-at-large-community-at-large-advisory-committee-alac-30-11-2022>
 10. “**INTA is pleased to provide our comments on 2 areas of the proposed recommendation.** These are found in Sections 2 and 10 of the report. In **Section 2, the recommendations do not accurately reflect the necessity and urgency of executing appropriate data protection agreements** to cover the data collection, processing, publication, transfer and access activities contemplated by the EPDP Phase 1 Policy. In **Section 10, the recommendations are indefinite as to the responsibilities of the contracted parties in evaluating requests for access to information.** Further, the recommended response times are unduly long and burdensome on the requestor who endeavors to act quickly on suspected cases of abuse. INTA requests that the drafters of the policy reconsider these sections based on INTA's specific observations so that the system will be consistent, predictable and more user friendly.” (INTA) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/constituency-intellectual-property-05-12-2022>
 11. “**The final NIS2 text was adopted by the European Parliament on 10-Nov-2022. The BC and other members of the EPDP frequently cited pending NIS2 regulation in our advice to create evolution mechanisms for registrant data policy.** Unfortunately, the EPDP Working Group and GNSO Council did not follow that advice. **NIS2 now requires EU Member States to enact regulation that may render some EPDP policy recommendations in conflict with law.** Specifically, **NIS2 requirements to publish registrant data for legal persons, requirements to maintain accurate registrant data, and potentially requirements for registries to maintain registrant data (i.e. Thick Whois).**The **BC therefore recommends that implementation of EPDP Phase 1 and Phase 2 be reassessed after the first EU Member State implements regulations pursuant to NIS2.**” (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/icann-business-constituency-bc-05-12-2022>
 12. “The IRT to produce the proposed Registration Data Consensus Policy for gTLDs should be implement as soon as possible by the community.” (BC) <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/business-constituency-01-12-2022>

-
13. “In August 2022, ICANN published its Draft Registration Data Policy, requesting feedback from the community. We note that ICANN published the Draft Registration Data Policy as an outcome of the work of the Implementation Review Team (IRT) to develop an implementation plan in line with the Consensus Policy Implementation Framework (CPIF), which was previously developed by ICANN and adopted by the GNSO Council.

We welcome the work of ICANN to release the document in line with [Workstream 2 Recommendations on ICANN Transparency](#). Our analysis shows that, primarily, **the document is a good first step but has fundamental gaps in ensuring the full implementation of Section 27.2 of the ICANN Bylaws (on Human Rights) and other Bylaws with an impact on human rights. CCWP-HR, therefore, urges ICANN to implement the recommendations below**, which would ensure that the Draft Registration Data Policy is implemented more closely with international law and best practice.”

Comments on the lack of clear timelines

The **draft policy states** that the effective date of the policy shall be “***no later than [540 days after the date of policy announcement and legal notice for implementation]***”. However, the call for **Public Comment that accompanies the draft Policy states: “after the implementation plan has been finalized, ICANN’s Contracted Parties will be notified of the implementation and compliance deadlines.”** We recommend that **the language in both documents be changed to either specify an exact date or ensure that the language is consistent, so that all stakeholders have clarity and legal certainty.** Given that the draft policy aims to further enhance the privacy of registrants, **we recommend that the deadline for compliance be made as soon as practicable (preferably within the first 6 months)**, as any further delay in securing the rights to privacy of registrants puts their data at risk.”

Comments on the requirements for Data Protection Agreements

We welcome the requirement that “**ICANN, gTLD Registry Operators, and accredited Registrars MUST enter into required data protection agreements** with each other and with relevant third party providers contemplated under this Policy where applicable law requires. The terms may include legal bases for processing Registration Data.”

We recommend that the requirement be made more robust to **additionally include mandates on ICANN, gTLD registry operators and accredited registrars to conduct full human rights impact assessments (HRIAs) or data protection impact assessments (DPIAs), carried out by independent experts, within one year after the compliance deadline and at least every two years thereafter.**

HRIAs and DPIAs are activities that include engaging in consultation with both internal and external stakeholders of an entity. This is done so that the entity can accurately determine the potential and actual effects of their corporate policies,

practices, products, and services on human rights and data protection, respectively, and then take steps to lessen the effects of any adverse effects. The HRIA has been acknowledged by ICANN itself as a methodology through which it can comply with its commitments as outlined in Section 27.2 of the ICANN Bylaws (on human rights) as well as in the Framework Of Interpretation for Human Rights (FOI-HR).

Under the United Nations Guiding Principles (**UNGPs**) on Business and Human Rights, companies including ICANN, gTLD registry operators and accredited registrars are responsible for respecting the human rights of their stakeholders and customers. Conducting HRIAs and DPIAs will ensure that these companies are not only in compliance with international human rights standards and principles, but also with their national and regional obligations, such as those under the European Union General Data Protection Regulations (**GDPR**).

Comments on the requirements for Collection of Registration Data

Under Section 6.7 and the Implementation Notes of the draft policy, there is leeway for gTLD registry operators, and accredited registrars to a) collect data in addition to the data provided for under the draft policy and b) process data for purposes that are beyond the scope of this draft policy.

We recommend that these sections be redrafted to require ICANN registries and gTLD registry operators to a) obtain the express consent of Registrants before the collection of data and b) clearly inform registrants of what data is required and not required to be collected under this draft policy, prior to obtaining registrant consent to collection.

Comments on the requirements for deletion of administrative contact data

We welcome the recommendation, which allows gTLD registry operators and accredited registrars to delete administrative contact data that was collected prior to the publication of the draft Data Consensus Policy but note that the drafting makes it optional by the use of “MAY” instead of “MUST”. We therefore recommend that this be redrafted to make it mandatory, unless the express, informed consent of the Registrant is provided or in the case of ongoing law enforcement processes at the time of the policy's publication.

Comments on Disclosure Requests.

We welcome this section, as it requires that, when providing responses to disclosure requests, gTLD registry operators and accredited registrars' responses must provide an explanation of how the fundamental rights and freedoms of the data subject were weighed against the legitimate interest of the requestor (if applicable).

However, this provision applies as a response to a third-party requester for data and does not clearly allow for the involvement of registrants in decisions

involving their data. The lack of provisions for notifying registrants when requests to access their registration data are made undermines their ability to challenge these requests. As such, this mechanism does not adequately balance the needs of a third-party requester for access to information with registrants' rights to privacy and data protection.

To ensure compliance with the principles of necessity, proportionality, and the requirement for due process under the international human rights framework, **we advise that users and registrants be provided with an independent mechanism to appeal requests before their registration data is disclosed to third-party requesters.**

Conclusion

CCWP-HR is grateful to have participated in this public comment process in accordance with the November 2019 ICANN Board approval of the FOI-HR. We welcome feedback on any aspect of this initiative and extend an open invitation to any interested individuals to get involved in the next phase of work. To become a member of the Cross-Community Working Party on ICANN and Human Rights (CCWP-HR), visit the CCWP-HR page on the ICANN Community website. **(CCWG)** <https://www.icann.org/en/public-comment/proceeding/registration-data-consensus-policy-for-gtlds-24-08-2022/submissions/cross-community-working-party-on-icann-and-human-rights-ccwp-hr-05-12-2022>.

Section 4: Analysis of Submissions

Overall, comments received remained positive, with key themes centered around providing additional or clarifying language to address ambiguities identified within the Registration Data Policy, as well as the importance of completing and publishing the Data Processing Agreements. In addition, several comments centered on topics including:

- Requirements relating to the transfer of specific registration data from registrar to registry and the impact on the Thick WHOIS Transition Policy for .COM, .NET and .JOBS. (See section 7 of Registration Data Policy.)
- Changes to processing requirements for administrative and technical contact data elements. (See section 6 of Registration Data Policy.)
- Changes to Disclosure Requirements. (See section 10 of Registration Data Policy)
- Ensuring the Registration Data Policy is consistent with amended RA and RAA agreements.
- The recent adoption of The Network and Information Security (NIS2) Directive.

ICANN Org values the opportunity to receive comments from the ICANN community and thanks those who participated in this proceeding. ICANN org will consider the input received and update the draft Registration Data Policy and Redlined policies as needed.

Section 5: Next Steps

ICANN org will continue to analyze the input received and will work with the Implementation Review Team (IRT) to review and consider updates to the draft Registration Data Policy, as needed. When this is completed, a record of all comments and how they were taken into account will be added as an addendum to this report and made available on the [Registration Data Policy wiki page](#).

ICANN's contracted parties will be notified of the implementation/compliance deadlines once any relevant areas of the Registration Data Policy for gTLDs Consensus Policy are updated, and implementation documents are published.

ICANN org Review of Public Comments

Registration Data Consensus Policy for gTLDs

ICANN org
28 April 2023



TABLE OF CONTENTS

1. Introduction:	3
2. Major Themes of comments received:	3
1. Public Comments regarding Data Protection Agreements (DPA)	3
2. Public Comments regarding the recent adoption of the Directive on measures for a high common level of cybersecurity across the Union (the “NIS2 Directive”)	4
3. Public Comments regarding Thick WHOIS	4
4. Public Comments regarding the “Reseller” Field	5
5. Public Comments regarding Response Times to Urgent Requests to Disclose non-public Registration Data	5
6. Public Comments that were determined to be out of scope for the Registration Data Policy	6
3. Specific Comments that resulted in changes to the draft Registration Data Policy and/or Redlined Policies and Procedures:	7
4. Specific Comments considered that did not result in changes to the draft Registration Data Policy and/or Redlined Policies and Procedures	9
3.1 Input suggesting Additional Clarifications	9
Section 3: Definitions and Interpretation	9
Section 6: Collection of Registration Data	9
Section 7: Transfer of Registration Data from Registrar to Registry Operator	10
Section 10: Disclosure Requests	10
Section 12: Retention of Registration Data	10
Addendum I	11
3.2: Input suggesting the draft Policy Language Does Not Accurately Reflect the Policy Recommendations	11
Section 2: Scope	11
Section 3: Definitions and Interpretation	12
Section 4: Policy Effective Date	13
Section 5: Data Protection Agreements	13
Section 6: Collection of Registration Data	14
Section 8: Transfer of Registration Data to Data Escrow Providers	16
Section 9: Publication of Domain Name Registration Data	16
Section 11: Log Files	16
Section 12: Retention of Registration Data	16
3.3 Input suggesting Additional Concerns with the draft Policy language in Registration Data Policy	17
Section 6: Collection of Registration Data	17
Section 9: Publication of Domain Name Registration Data	18
Addendum I	19

Addendum II	19
Background	20
3.4 Input suggesting Policies and Procedures were Incorrectly Redlined	20
3.5 General Comments	27

1. Introduction:

ICANN org appreciates the chance to gather feedback from the ICANN Community and expresses gratitude to those who participated in the Registration Data Policy public comment proceeding. ICANN Org's EPDP Phase 1 Implementation project team (IPT) carefully reviewed and considered all input received and organized comments into the following sections:

- Major Themes of comments received
- Specific Comments that resulted in changes to the draft Registration Data Policy and/or Redlined Policies and Procedures
- Specific Comments considered that did not result in changes to the draft Registration Data Policy and/or Redlined Policies and Procedures

2. Major Themes of comments received:

1. Public Comments regarding Data Protection Agreements (DPA)

- a. The IPT received input in several comments regarding:
 - i. The length of time required to complete negotiations of the recommended Data Protection Agreements,
 - ii. Lack of clarity around the obligations and roles of each party entering the Data Protection Agreements,
 - iii. Whether the draft policy language remained consistent with the EPDP Phase 1 policy recommendations, because recommendation 19 requires contracted parties to enter into DPAs, as appropriate.
 - iv. The agreements' impact to the Thick WHOIS Policy,
 - v. The desire for an update method for the DPA once published.
- b. The IPT acknowledges the concerns raised regarding the recommended Data Protection Agreements. Many segments of the community, in this public comment proceeding and elsewhere, have emphasized that negotiations between ICANN org and the contracted parties must be finalized and additional information about the results of this negotiation must be shared with the broader community as a matter of urgency. ICANN org and the contracted parties house negotiation group have been negotiating to find an acceptable solution for all parties involved, but have not yet agreed on a resolution to a few, final issues. The IPT will share a draft when the negotiations are complete. For clarity and transparency, the IPT can confirm that any template agreement negotiated and agreed to by ICANN and the contracted parties house negotiation group to implement the EPDP Phase 1 recommendations will include the Purposes for processing gTLD Registration Data as identified in Recommendation 1 of the EPDP Phase 1 working group.
- c. The IPT respectfully disagrees with the suggestion that any changes to the DPAs entered into between ICANN and a contracted party would require public comment, as this is an

agreement between two parties, rather than a Consensus Policy. Regarding obligations and responsibilities, the IPT notes that the EPDP recommendations stated that the parties must enter required data protection agreements as appropriate. To clarify, the recommendations did not require that each contracted party must enter into a data protection agreement with ICANN or that the registries must have a DPA with each registrar they work with.

Section 5 of the Registration Data Policy sets out that either the registry or registrar may choose to request a DPA, specifically noting, *“If Registry Operator or Registrar determines that such agreements are required by applicable law, it MUST make the request without undue delay pursuant to this policy.”*

Regarding the impact of the DPA on the Thick WHOIS Policy, the draft Data Processing Specification currently being discussed between ICANN and the contracted parties would have no impact on a registry’s obligation to transfer contact data (or lack thereof). This is a policy requirement, rather than a matter to be addressed in the draft Specification.

2. Public Comments regarding the recent adoption of the Directive on measures for a high common level of cybersecurity across the Union (the “NIS2 Directive”)

- a. The IPT received input in several comments regarding:
 - i. The newly adopted NIS2 Directive and its impact on the proposed Registration Data Policy, including input regarding the Thick WHOIS Policy and the EPDP Phase 1 recommendations on transfer of registration data.
- b. The IPT would like to clarify that, absent a conflict that would prevent a contracted party from complying with both local law and an ICANN Consensus Policy, requirements under local law have no direct impact on ICANN policy requirements. It is possible (and indeed, likely under NIS2) that some contracted parties will be required to take steps in addition to those required by the Policy, but these are laws, rather than ICANN policies. As such, they are enforced by local regulators and courts, not ICANN. The EPDP Phase 2a team made a [policy decision](#) not to require the contracted parties to take different measures related to the data of legal persons, which was approved by the GNSO Council and adopted by the Board. If the ICANN community wishes to modify policy requirements in light of changes in law, there are mechanisms to do so (e.g. the consensus driven, bottom-up, multi stakeholder policy development process).

3. Public Comments regarding Thick WHOIS

- a. **The IPT received a large amount of input from the ICANN community regarding the Thick WHOIS Policy**
 - i. The IPT would like to clarify that the policy language regarding the transfer of registration data from registrars to registries was discussed extensively and is consistent with guidance from the GNSO Council and Board direction. The incorporated implementation notes were included to make clear how this provision would be enforced by ICANN org. Specifically, within the draft Registration Data Policy, the decision regarding whether a registry will receive

the “additional” data or not will depend on the registry and registrar determining the legal basis for the transfer and entering into a data protection agreement that covers the data, where these are required by law.

After receiving input from the GNSO Council, The IPT, in consultation with the Implementation Review Team, concluded that ICANN org could enforce a transfer requirement only if the relevant contracted parties agree that a legal basis exists for the transfer and a data protection agreement is in place. If additional requirements for the transfer of registrant contact data from registrars to registries apply to the parties under local laws, such local laws may be considered by the contracted parties when determining whether a legal basis exists for the transfer of registration data from registrar to registry. However, ICANN’s role is limited to enforcing ICANN policies and agreements and does not extend to enforcing local laws.

4. Public Comments regarding the “Reseller” Field

- a. The IPT received various inputs concerning the option to collect, transfer, and publish the reseller field.
 - i. After careful consideration of the public comments received, the IPT determined that additional changes should not be made to the policy language pertaining to the requirements related to the reseller field. There is no indication that the draft policy was drafted incorrectly, and the EPDP Phase 1 team determined that the collection, transfer, and publication of the reseller field remain optional. The draft policy language maintains the status quo as org recognizes that current business practices allow for the optional collection, transfer, and publication of the reseller field. Thus, the IPT believes that making any recommended changes is beyond the scope of the policy as it would create additional changes that are not required by the EPDP Phase 1 recommendations.

5. Public Comments regarding Response Times to Urgent Requests to Disclose non-public Registration Data

- a. The IPT received a large amount of input concerning the definition of urgent requests and asserting that the draft Registration Data Policy failed to implement expedited timeframes consistent with the urgency required to respond to urgent requests.
 - i. The IPT acknowledges the concerns raised regarding the time period allotted to respond to urgent requests for disclosure of registration data. After careful consideration and taking into account the feedback received, the IPT believes there is sufficient justification to revisit the policy language and to require a 24-hour response time for urgent requests. The IPT believes that the 24-hour response time accurately reflects the intent of the EPDP policy recommendations, particularly in cases where urgent requests rise to the level of emergencies and are made to prevent harm to individuals or critical infrastructure, such as those related to threat to life, human life and child exploitation. The 24-hour time period allows urgent requests to be addressed sooner to prevent harm through identifying the perpetrator for the disruptive action or the victim for notification or both. The IPT also notes that the draft

Registration Data policy language includes a narrow definition of what constitutes an "urgent request", which only applies to circumstances that pose an imminent threat to life, of serious bodily injury, to critical infrastructure, or of child exploitation. The limited definition presents a high threshold and minimizes the likelihood of Registry Operators/Registrars receiving requests that meet the standard of urgent frequently or in a high volume. Furthermore, the IPT removed the term "business days" from the response time requirement, as it is subject to different interpretations in different regions, and is not required by the EPDP Phase 1 team as the term "business days" appears in brackets in the Final Report. This change will help to ensure that acknowledgments are provided within the intended timeframe of 24 hours rather than potentially extending beyond 2 calendar days. Lastly, the proposed 24-hour time period aligns with Section 3.18.2 of the 2013 RAA which *"requires registrars to maintain a designated abuse point of contact to receive reports of abuse involving illegal activity by law enforcement, consumer protection, quasi-governmental or other similar authorities. Registrars must review well-founded reports of illegal activity submitted to the contact within 24 hours by an individual who is empowered to take necessary and appropriate actions in response to the report."* Specifically, registrars already are required to have a Law Enforcement Agency (LEA) abuse contact that must review reports of abuse involving illegal activity within 24 hours, thus Registrars could leverage that type of contact which is already in place.

6. Public Comments that were determined to be out of scope for the Registration Data Policy

- a. The IPT received several comments on areas which, following further review, were determined to be beyond the scope of this implementation, as the EPDP Phase 1 did not include recommendations to support the following suggestions:
 - i. The expansion of the scope of the Registration Data Policy, because the scope of the Registration Data Policy is strictly limited to the processing activities listed in the policy.
 - ii. Inclusion of requirements related to costs and mechanisms to disclose Registration Data, specifically;
 1. Ensuring disclosure requests are free of charge
 2. Providing criteria for contracted parties to determine whether or not to disclose Registration Data.
 3. Independent mechanisms for users and registrants to consent to disclosure of data and gain clarification of what data is or is not required to be collected under the Registration Data Policy.
 4. Providing an independent mechanism to notify users and registrants of requests for access to nonpublic registration data, as registrars and registries will likely have notification requirements based on jurisdictional law.
 5. Mechanism to inform users of a location and process for submitting disclosure requests. Inclusion of a direct link to a page where the

mechanism and process for submitting Disclosure Requests is detailed in the policy.

- iii. Defining which entities should or should not be considered “Resellers” to the extent entities exist within the registrar distribution channels.
- iv. Inclusion of public identifiers in the draft policy to improve accountability and protect natural person’s data.
- v. Substitution of “technical contact” for the “administrative contact” within Transfer Policy.
- vi. The distinction between legal and natural persons.
 1. The IPT further clarifies that the draft Registration Data Policy requirements do not explicitly distinguish between the registration data of legal and natural persons, because, as a matter of policy, the ICANN community determined not to require contracted parties to take different measures related to the data of legal persons. However, the EPDP Phase 2a recommendations allow contracted parties the option to include additional data elements which may be used to distinguish between legal and natural persons.

3. Specific Comments that resulted in changes to the draft Registration Data Policy and/or Redlined Policies and Procedures:

The IPT appreciates the comments received from the community which resulted in the following changes in the draft Registration Data Policy:

1. Introduction

- a. The IPT received input suggesting that section 1 should include the defined term of “processing”.
 - i. Following further review, the suggested changes were made to section 1 of the policy to describe that the Registration Data Policy applies to all aspects of registration data.

2. Section 2: Scope

- a. The IPT received input suggesting the language “other purposes” in Section 2 of the policy would benefit from further clarity.
 - i. Following additional review, the IPT determined that the language “other purposes” created confusion related to purpose and intent of the language. For clarity, the language “*Registry Operator’s and Registrar’s Processing of Personal Data contained in Registration Data for purposes other than the purposes identified in the Data Protection Agreement required by Section 5 is beyond the scope of this Policy*” was incorporated into Implementation Note A, as it directly relates to the processing described in the Implementation Note.

3. Section 3: Definitions and Interpretation

- a. The IPT received input noting that the definition of “Urgent Request” contained a grammatical/semantic error.
 - i. Following additional review, the IPT made the suggested changes in section 3.8 of the draft policy.

- b. The IPT received input suggesting that section 3.10 should be deleted because it was inconsistent with contract drafting principles.
 - i. The IPT conducted a comprehensive review of every time “or” is used throughout the draft policy to determine whether requirements would change without this definition and determined that this section could be deleted. In order to avoid impacts to the requirements of the policy as a result of deleting section 3.10, minor grammatical changes were made in several sections of the policy as identified in the redline.

4. Section 9: Publication

- a. The IPT received input suggesting that section 9.2.1 in the draft policy should be split into subsections for added clarity.
 - i. Following further review, the IPT agreed that the suggested changes will add clarity and incorporated the changes to the draft policy.
- b. The IPT received input noting that section 9.2.4 should clarify that registrars provide the opportunity for the RNH to consent to publication. Following further review, the IPT included the suggested clarification in the implementation notes of the draft policy.

5. Section 10: Disclosure Requests

- a. The IPT received multiple inputs from the community noting that the urgent requests response period in the draft policy did not accurately reflect the importance of “urgent requests”.
 - i. Following further review, the IPT believes that requiring a 24-hour response time for urgent requests accurately reflects the nature of “urgent requests”, particularly those that present potential harm to individuals, such as threat to life, of serious bodily injury and of child exploitation. Thus, section 10.5 of the draft policy was updated to reflect this urgency. Please see section 3 for additional information regarding the input received on response times to urgent requests for disclosure.

6. Background

- a. The IPT received input noting the background section of the draft policy should reflect important considerations of the EPDP Phase 1 team including the publication of its Final Report.
 - i. Following further review the IPT has incorporated the suggested changes to the background section of the draft policy.

7. URS Procedure

- a. Following the review of the input received on the redlined URS Procedure, the IPT included a footnote in section 4.2 which clarifies the term “Registration Data”, which is meant to have the same meaning as it is given in the Registration Data Policy.

4. Specific Comments considered that did not result in changes to the draft Registration Data Policy and/or Redlined Policies and Procedures

3.1 Input suggesting Additional Clarifications

Input Received	Implementation Project Team Response
Section 3: Definitions and Interpretation	
<p>3</p> <p>“Unless there is a compelling reason, all definitions in the policy should reside in this section. For example, Section 9.2.2. Defines “Redact”, and Implementation Note H defines “Creation Date”. For clarity, these definitions should be moved to Section 3.” (RySG)</p>	<p>In response to the RySG’s concerns regarding definitions residing outside section 3, the IPT clarifies that the definitions placed outside of Section 3 are not intended to be standardized throughout the draft policy language and are only applied to the appropriate sections based on their specific requirements. For example, Section 9.2.2, which defines redaction, is only applied in the manner as specified in section 9.2.2</p>
Section 6: Collection of Registration Data	
<p>6.3</p> <p>“The RrSG notes that recommendation 6.3 applies only at the time of registration, and suggests that to ensure PII is not inadvertently disclosed publicly, that these requirements also apply when technical contact information is updated. The RrSG is also concerned that registrars may not have a direct relationship with the technical contact, and may not be able to properly obtain consent to display PII. The IRT should resolve this ambiguity.” (RrSg)</p>	<p>To address the concerns raised regarding properly obtaining consent to display PII, the IPT will provide further clarification in its educational materials, which will be available once the Registration Data Policy is published.</p> <p>Additionally, the IPT notes that it is up to each individual registrar to determine the appropriate methods to obtain consent to display personal data based on the registrar’s individual jurisdiction, business model, and legal obligations.</p>
<p>6.7</p> <p>“The RySG is aware that the global legislative environment continues to evolve and believes that a slight addition to Section 6.7 would add clarity to what is allowable as part of this section. Suggested amendment (additional text between **): 6.7. Registrar MAY collect additional data elements as required by its Registry-Registrar</p>	<p>The IPT notes that as registrars and registries are required to abide by applicable laws and regulations (pursuant to both the law and the underlying ICANN agreements), the IPT believes the additional language is not necessary for additional clarity.</p> <p>The IPT also notes that the underlying principle that ICANN policy should not create a conflict with applicable law is consistent with Section 1.2 of ICANN’s Bylaws, which</p>

	<p>Agreement and/or the Registry Operator’s Registration Policy, **including if required by law**” (RySg)</p>	<p>requires that ICANN “carry out its activities in conformity with relevant principles of international law and international conventions and applicable local law.”</p>
<p>Section 7: Transfer of Registration Data from Registrar to Registry Operator</p>		
<p>7.2</p>	<p>“The RrSG notes that while recommendation 7.2 refers to “Registrar Whois Server”, concurrently the RA and RAA are being amended to primarily replace whois obligations with RDAP requirements. While registrars may continue to provide whois service after the transition from whois to RDAP, the recommendations should include a reference to this change to avoid future ambiguity.” (RrSG)</p>	<p>The IPT would like to note that while the draft policy does not specifically reference the amendments in process, the policy accounts for this logic within the collection section to account for updates that will be made to the RAA and RA, which will then flow to other processing requirements. Furthermore, the IPT provided its rationale in Drafting error 2.4 which notes “Registrar Whois Server” value is only required to be generated if required by the Registrar Accreditation Agreement or ICANN Consensus Policy.</p>
<p>Section 10: Disclosure Requests</p>		
<p>10.1</p>	<p>“Section 10. Requires “Registrar and Registry Operator MUST publish on their homepage a direct link to a page where the mechanism and process for submitting Disclosure Requests is Detailed”. The relevant source recommendation, Recommendation 18, refers to the fact that “Registrars and Registry Operators must publish, in a publicly accessible section of their website, the mechanism and process for submitting Reasonable Requests for Lawful Disclosure”. The policy recommendations deliberately do not use the word “homepage” as this is not always the best or most appropriate place to provide the link. Some flexibility should be given to Registrars and Registry operators to make that determination. (RySG)</p>	<p>While drafting the policy language, the IPT received feedback from the IRT noting the difficulty in locating information regarding disclosure requests. After careful consideration, the IPT determined that maintaining the term “homepage” would benefit those seeking to submit disclosure requests, for registrars’ and registry operators’ websites to have a designated location that provides a direct link to a page where mechanisms and processes to submit disclosure requests are available OR reside.</p>
<p>10.6</p>	<p>“10.6 uses the ambiguous term “business days” and should rather specify that it is the registrar's business days that are relevant. Tucows' Recommended Language for Section 10: <i>For Urgent Requests for Lawful Disclosure, Registrar and Registry Operator MUST acknowledge and respond without undue delay, but no more</i></p>	<p>The IPT acknowledges that the term "business days" includes certain ambiguities. However, the IPT discussed this topic at length with the Implementation Review Team (IRT) and determined that the "business days" provision should refrain from incorporating interpretations subjective to contracted parties as it would create further ambiguity for users who request access.</p>

	<i>than two (2) business days (as determined by the recipient) from receipt.” (Tu cows)</i>	
--	---	--

Section 12: Retention of Registration Data

12	“Rec #15 arrived at 18 months as an “interim” retention period. The final determination of retention period may be longer, based on legitimate purposes identified through community consultation.” (BC)	The IPT notes that the retention period in the Registration data policy represents the minimum period identified for which data must be retained for Transfer Dispute Resolution Policy (TDRP) purposes. Contracted parties must determine themselves the appropriate retention period for data retained beyond this required period.
-----------	---	---

Addendum I

	“While this section accurately reflects the Policy Recommendation language, we think it could be more clear . Tu cows’ Recommended Language for Addendum I: Note: this Addendum I applies to contracted parties providing WHOIS (available via port 43) or web-based Whois directory services only if required by the Registrar Accreditation Agreement or ICANN Consensus Policy.” (Tu cows)	After further review, the IPT determined that Addendum I does not require further clarification. The Educational Materials will be available for implementers to review once the Registration Data Policy is published. The IPT also encourages reviewing the RDAP amendments in the RAA & RA for additional clarity.
--	--	---

3.2: Input suggesting the draft Policy Language Does Not Accurately Reflect the Policy Recommendations

Input Received

Implementation Project Team Response

Section 2: Scope

2.2	“ Section 2.2 is incorrect and inappropriate as drafted. This policy’s scope is not limited to only the purposes listed in yet to be created Data Protection Agreements “DPA” (and assuming agreements are in place, they would be subject to change over time). The scope of this policy clearly includes the following processing, notwithstanding the existence of further Data Protection Agreements: collection;	The IPT clarifies that each section of the draft Registration Data Policy addresses the topics of collection, processing, publication, and disclosure. Thus, the inclusion of the suggested topics in Section 2.2 is not required. For added clarity, the reference to “other purposes” in the draft section 2.2 posted for public comment has been moved to Implementation note A.
------------	--	---

	<p>processing; publication; and, importantly, disclosure to third parties as required by this policy and/or governing law. The absence of required DPAs has put numerous initiatives at ICANN in limbo. This certainly true for any type of program that contemplates data management and access. The IPC reiterates the urgency of ICANN completing negotiations with the Contracted Parties to facilitate data processing and data access to the benefit of the entire multistakeholder community.” (IPC)</p>	
--	---	--

Section 3: Definitions and Interpretation

<p>3.9</p>	<p>“Delete 3.9, or specifically call out the definitions in those agreements since there may be contradictions or unintended consequences. For example, the terms "natural person" and "legal person" are not defined. While these terms often have standard meanings in a country's laws, those standard meanings differ from country to country. To facilitate better compliance with privacy regulations in the future, these terms should be defined.” (BC)</p>	<p>Regarding section 3.9 which notes <i>“Terms capitalized but not defined in this Policy SHALL have the meaning given to them in the Registry Agreement or Registrar Accreditation Agreement, as applicable”</i>, the IPT notes that this only applies to the terms capitalized within the draft Registration Data Policy.</p> <p>Legal person and natural person are not capitalized or defined in the policy, as the EPDP Phase 1 team did not require defining the terms “legal” and “natural” as part of policy. Additionally, the terms “legal” and “natural” persons may be defined differently based on applicable laws and regulations in different jurisdictions..</p>
-------------------	---	--

<p>3</p>	<p>“The GAC acknowledges the role of the GDPR in serving as a catalyst for this policy and notes that the precise wording of these definitions has no bearing on parties’ obligations to comply with applicable law. Nevertheless, the GAC recommends that in some circumstances greater specificity could be useful, including on “consent” (the GDPR requires the provision of consent for each purpose.) and “personal data,” which would benefit from greater clarity around the meaning of an identifiable natural person. Further, the GAC recommends the addition of text making clear that no costs will be borne by those willing to access “published” data. Finally, while the GAC is cognizant of maintaining a narrowly tailored set of circumstances warranting “urgent requests for lawful disclosure,” to ensure contracted parties are able to respond efficiently to these requests, the GAC recommends that this category of urgent requests include “imminent or ongoing serious</p>	<p>The IPT acknowledges the benefit of clarifying certain terms in the draft Registration Data Policy and would like to note the use of the terms “personal data” and “consent” are consistent with how they are used in the EPDP Phase 1 policy recommendations. Additionally, the IPT decided against incorporating the clarification regarding costs borne to those who request access into the draft policy language as it goes beyond the scope of the EPDP Phase 1 recommendations.</p>
-----------------	---	---

cybersecurity incidents” (such as those deriving from large scale ransomware, malware or botnet campaigns, which may for example affect consumer protection and would require an immediate need for disclosure) **regardless of whether the target is critical infrastructure.”** (GAC)

Section 4: Policy Effective Date

4 “The EPDP Final Report called for implementation of the recommendations one year from the Report (which was published in 2019 (almost three years ago). **There is no reason that the EPDP’s recommended proposed timeline for implementation should be ignored. By the time** the final policy documents are approved and **the 18 month period begins to run, it will likely be implemented in late 2024, which will be over 5 years from the Final Report**, which is highly **problematic for an expedited policy process.”** (BC)

Regarding implementation timing the IPT would like to reiterate several challenges faced during the Expedited Policy Development Process (EPDP), e.g., interaction with evolving legislation and legal guidance, time pressure, have also carried over and impacted the implementation work. Some of the factors affecting the progress of the implementation work have included: (a) Several recommendations were subject to varying interpretations and in some cases were escalated, using established processes, to the Board and GNSO Council to help resolve. An example of an escalated case is Recommendation 12 regarding the deletion of the Registration Organization Field which required the Board to adopt the [GNSO Council supplemental guidance](#), which was not reached until [24 February 2022](#). (b) The implementation of the Registration Data Policy required an impact analysis of all existing consensus policies, often requiring multiple reviews and further updates to related policies. (c) The implementation work also adjusted to include the expanded scope of the EPDP Phase 2 Priority 2 recommendations which required analyzing and incorporating a new set of Board adopted policy recommendations. Each of the factors mentioned played a role in extending the Phase 1 implementation timeline due to their unique levels of complexity. Lastly, the IPT consulted with the contracted parties to determine the amount of time required to implement the Registration Data Policy and no concerns were raised when the IPT discussed the [proposed](#) 18 month implementation timeline with the IRT.

4 “The EPDP Recommendations were issued in February 2019 and expected to be approved by the GNSO and Board in short order. The EPDP team (including representatives of contracted parties) understood that it would take some time to translate the recommendations in to policy and then to have contracted parties implement that policy. Accordingly, **Recommendation 28 extended the validity of terms within the Temporary Specification to allow for the creation and implementation of the policy.** After due consideration **the EPDP team set a deadline for contracted party compliance** at 29 February 2020 (**1 year after issuance of the Phase 1 report**). Clearly the EPDP team underestimated the amount of time needed to translate the recommendations into policy. However, **the EPDP team, including registry and registrar representatives unanimously believed that the allowed period was sufficient for contracted party implementation.** Given Recommendation 28, and the fact that these recommendations are reasonably consistent with the Temporary Specification, and that the differences have been well known now for several years, the

	ALAC believes that allowing an additional 18 months for contracted party implementation is excessive and uncalled for. (ALAC)	
--	---	--

Section 5: Data Protection Agreements

5	<p>“We strongly urge ICANN to collaboratively finalize and then sign the DPA which has been in discussion for several years. The language in the Draft Registration Data Consensus Policy is ambiguous where the Recommendations of the EPDP Phase 1 are not. For example, the Draft Registration Data Consensus Policy says “relevant third party providers” but does not indicate who can designate third party providers as “relevant”. The EPDP Phase 1 Recommendations clearly intended Contracted Parties to be able to designate third party providers, both to themselves and to ICANN, as “relevant”. Further, ICANN MUST enter into data protection agreements with Data Escrow Providers but the language in the Draft Registration Data Consensus Policy allows ICANN to avoid this requirement because of its linguistic ambiguity. Tucows’ Recommended Language for Section 5: <i>If Registry Operator or Registrar determines that such agreements are required by applicable law, Registry Operator and Registrar MUST make the request without undue delay pursuant to this policy for data protection agreements between the Contracted Party and ICANN and for data protection agreements between ICANN and a relevant third party provider. ICANN MUST without undue delay enter into data protection agreement or agreements upon such request.</i>” (Tucows)</p>	<p>The IPT notes that the language in section 5 of the draft policy was discussed at length with the IRT. After careful consideration of the input provided, the IPT is unable to include this addition into the policy as it includes additional requirements which are outside the scope of the EPDP phase 1 recommendations.</p>
---	--	---

Section 6: Collection of Registration Data

6.1	<p>“In 6.1, Registrars should not have an option to exclude the Organization Field when collecting registrant data, since it is a mandatory field for any registrant that is an Organization. As a result, 6.1 needs to be updated to require Organization after the Name Field. In 6.1, Registrars should not have an option to exclude</p>	<p>The IPT acknowledges the concerns raised regarding section 6 of the draft policy and notes that these topics were discussed at length with the IRT to assist in drafting the policy language in line with the EPDP Phase 1 recommendations. For further clarification, regarding input on the exclusion of the technical fields, the IPT would like to note the policy recommendations identify the technical fields as optional for</p>
-----	--	---

	<p>Technical Fields, since it is a mandatory field if the registrant elects to provide it. As a result, 6.1 must be updated to require these fields as reflected in the table in the Phase 1 Final Report. The Reseller Field also is required to be listed in the fields collected by the Registrar in 6.1, as was clear in the EPDP Phase 1 Final Report. Reseller can be left blank if the Registrar does not use resellers. But reseller data needs to be processed if the data is provided, per the Final report in the footnote where it says “In both cases, if data is provided, it must be processed.” (Footnote 7 on page 7 of the final report) The WHOIS Server field is also required and was not a drafting error as suggested by the Report: ““Registrar Whois Server” value is only required to be generated if required by the Registrar Accreditation Agreement or ICANN Consensus Policy.(See“Drafting Error” 2)” This element needs to be preserved. As a result, the last sentence of 6.1 must be deleted. Indeed the sentence is inconsistent since it states that “Registrar Whois Server” value is only required to be generated if required by the Registrar Accreditation Agreement or ICANN Consensus Policy.(See“Drafting Error” 2).” Since the EPDP Phase 1 Final Report IS creating a consensus policy, it’s obvious that the Registrar WHOIS Server IS now a requirement going forward since the Final Report correctly lists the Registrar WHOIS Server as a requirement in the table for Recommendation 5.</p> <p>Regarding the deletion of the Administrative Contact, we note that implementing this change will violate the newly adopted NIS2 language which requires the collection of specific data in Article 28, Section 2 including: <i>“the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.”</i> As a result, the Consensus Policy should also require the collection, transfer and disclosure of the Administrative Contacts.” (BC)</p>	<p>registrars to offer and for the registered name holder to provide, therefore the policy language was drafted to note that the technical field is optional for the Registered Name Holder to complete (and <u>if</u> the Registrar provides this option). Additionally, the IPT clarifies that Recommendation 12 specifically notes that the “Registrar MUST provide the opportunity for the Registered Name Holder to provide values for the following data elements. If provided by the Registered Name Holder, Registrar MUST collect the following data element values: ... Registrant Organization”. The policy recommendation (Recommendation 5) allows the Registered Name Holder the option to provide a Registrant Organization value, which is subsequently how the policy language is drafted in section 6.1. Regarding the concerns for resellers, please see Section 2.4 above regarding the requirements to collect, transfer, and publish the reseller field. Regarding input on the WHOIS server field, the IPT acknowledges the concern to preserve the “Registrar WHOIS server”, and confirms that the requirement to preserve this element remains within the RAA in the case RDAP in unforeseen circumstances were to fail. Lastly, regarding the input concerning the adoption of NIS2, the IPT provided its response above in Section 2.2 of the report.</p>
<p>6.3</p>	<p>“The “are to” language in Recommendation 5 does not use MUST language, so there is no binding policy language and 6.3 should be MAY.” (IPC)</p>	<p>Regarding the requirements listed in section 6.3 of the draft Registration Data Policy, the IPT notes that the language in Recommendation 5 of the Final Report indicates an optional rather than a mandatory requirement. Although the word “MUST” is not explicitly mentioned, the policy language indicates that if provided, Registrars are</p>

expected **"to advise the Registered Name Holder at the time of registration that the Registered Name Holder is free to (1) designate the same person as the registrant (or its representative) as the technical contact; or (2) provide contact information which does not directly identify the technical contact person concerned."**

Section 8: Transfer of Registration Data to Data Escrow Providers

8 "Section 8 does not accurately reflect the intent of the Registration Data Consensus Policy." (IPC)

The IPT is unable to consider this input as no alternative suggestion or explanation to supplement is provided.

Section 9: Publication of Domain Name Registration Data

9.1.1 "As suggested in the definition section, the GAC recommends clarifying that publicly available means accessible free of charge. The proposed change is as follows:
9.1.1 *'In responses to RDDS queries, Registrar and Registry Operator MUST Publish free of charge the following data elements:'*" (GAC)

The IPT acknowledges the suggestion to clarify that publicly available means "accessible free of charge", however EPDP Phase 1 team did not recommend the incorporation of such requirements in this Policy, this recommendation is beyond the scope of this implementation.

Section 11: Log Files

11.1.2 "11.1.2 should be **MUST** maintain log files to confirm relay of communications from requestor to tech email address. Rec #13 explicitly says "and which shall contain confirmation that a relay of the communication between the requestor and the Registered Name Holder has occurred" Additionally, all of the **log file requirements should be amended to allow logging of information that is not Personal Information.**" (BC)

The IPT emphasizes that based on its discussions and work with the IRT, the team made every effort to implement the draft policy language per the language in Recommendation 13. The IPT reiterates its explanation in the "[Drafting Errors document](#)", which clarifies that Recommendation 13 did not include requirements for logging communication with the Tech email. Rather, the recommendation requires establishing a mechanism to log the relay of communication with the tech email if registrars choose to log them and make them available for compliance purposes. As a result, the policy requirement includes the Tech email for logging only if it has been collected.

11.1.1-11.1.2 "As drafted, 11.1.1 and 11.1.2 are impossible for CPs to comply with in modern logging software. The redactions/removals called for are overly burdensome in their redaction requirements to the point where they actually **conflict with the rest of the good logging requirements in Section 11.** It is almost understandable if contents

	must not be logged, but a log that does not contain the sender or recipient would be useless to the community. " (IPC)	
--	---	--

Section 12: Retention of Registration Data

12	<p>“Registrar MUST retain those data elements necessary for the purposes of the Transfer Dispute Resolution Policy for a period of no less than fifteen (15) months following end of Registrar’s sponsorship of the registration or an inter-registrant (change of registrant) transfer of the registration.’ The GAC recommends reviewing this provision, which only sets a minimum (mandatory) retention period, whereas the requirement under the GDPR is to limit retention to the period necessary to fulfill the purpose of processing.” (GAC)</p>	<p>Based on its research, the IPT determined that the retention of Registration data needed for TDRP appears to be the longest minimum retention period among all the policy and contract retention periods. Additionally, the IPT notes that no restrictions prohibit data from being retained for more extended periods for processing activities that fall outside of ICANN requirements. Each contracted party is responsible for ensuring that its retention practices concerning this data are in compliance with their agreements with ICANN, this Consensus Policy, and applicable law.</p> <p>Regarding article 5 of the GDPR and data minimisation principles, the IPT clarifies that the retention period represents the minimum period identified for which this data must be retained for TDRP purposes. Beyond this minimum retention period, contracted parties must determine for themselves, taking into account the necessity for the data, applicable laws, and other factors an appropriate retention period if the data is retained beyond this required period.</p>
12	<p>“Section 12 only sets a minimum retention period of no less than fifteen (15) months. The Provision should be further reviewed considering article 5 of the GPDR and data minimisation principles.” (AFNIC)</p>	

3.3 Input suggesting Additional Concerns with the draft Policy language in Registration Data Policy

Input Received	Implementation Project Team Response
----------------	--------------------------------------

Section 6: Collection of Registration Data

6.3	<p>“6.3. The GAC finds this section unclear as it could imply that under certain circumstances the contact details of the technical contact may replace the contact details of the registrant. The present data policy should ensure that the contact details of both the registrant and the technical contact are collected.” (GAC)</p>	<p>The IPT notes the input regarding the collection of the registrant and technical contact details. The IPT will provide further clarification on how contact details of both registrants and technical contacts are collected in its “Educational Materials”, which will be available once the Registration Data Policy is published.</p>
-----	--	---

<p>6.5 - 6.6</p>	<p>“In such cases, the GAC would benefit from further clarification as to which data elements SHOULD be used for each category of entities existing in registrar distribution channels. If data elements do not currently exist for such entities, the GAC would view it as constructive to create and incorporate within the Consensus Policy such elements.</p> <p>6.5 – 6.6: “If provided by the Registered Name Holder, Registrar MUST collect the following data element values”. The GAC acknowledges that this wording stems from Recommendation 12 of EPDP Phase 1, however the GAC reiterates that these data elements may change as a result of pending policy recommendations, particularly the approved Phase 2A recommendations. EPDP Phase 2A has required the functionality of distinguishing between legal and natural persons and the GAC believes that such distinction has not been taken into account in the present Draft Policy. In particular, data such as ‘the registrant organisation’, though not essential for registrants who are natural persons, should nevertheless be collected when the registrant is a legal person. This information can thus be optional for natural persons but should be mandatory for legal persons. As the GAC has stressed on multiple occasions, personal data protection regulations, including the GDPR, apply to the processing of personal data of natural persons and not legal persons. Therefore, the contracted parties should collect and make data of legal persons publicly available. Additional safeguards may be considered for the case where the email address of a legal person contains personal data, in which case a functional email address can be published instead.” (GAC)</p>	<p>The IPT notes that it is unable to implement the suggestion to distinguish between data of legal and natural persons, as the EPDP Phase 2A policy recommendations were not assigned by the Board as part of the EPDP Phase 1 IRT scope. Additionally, the IPT clarifies that the EPDP Phase 2A team made a policy decision not to require the contracted parties to take different measures related to the data of legal persons which was approved by the GNSO Council and adopted by the Board.</p>
-------------------------	---	--

Section 9: Publication of Domain Name Registration Data

<p>9.1.1, 9.2.1, 9.2.6, 9.2.2.3</p>	<p>“9.1.10 These MUST be published if present/provided.</p> <p>The first MUST in 9.2.1 should be MAY - ICANN is in the business of enforcing policy requirements, not in the business of enforcing laws. In the fourth line of 9.2.1, the word MAY conflicts with the word</p>	<p>The IPT clarifies that as part of the EPDP deliberations to determine if the Temporary Specification complies with the GDPR, and as listed in the data element table in Recommendation 10, the EPDP Phase 1 team decided that Registrant Phone Ext, Registrant Fax, and Registrant Fax Ext data elements are not required to be published.</p>
--	---	---

<p>9.2.2.4</p>	<p>“requirements.” A different word should be used (“options”?) since ICANN clearly does not intend these to be requirements. The 9.2.1(i) and (ii) carve outs are unacceptable. Each of (i) and (ii) would render this portion of the policy unenforceable as they would permit contracted parties sole discretion to do as they please. Such an outcome would be unacceptable.</p> <p>9.2.6 insufficiently captures this as it does not explicitly require the registrar to offer the option.</p> <p>In Sections 9.2.2.3 and 9.2.2.4 - Registries should be required to publish if they have the Org and City data elements.” (IPC)</p>	<p>Therefore, the suggested elements are included as a “MAY” provision because they are considered additional data elements not required for publication.</p> <p>The conditions stated in section 9.2.1 (i) and (ii) were necessary to make the requirement work for all Registrars and Registry Operators. The enforcement would include verifications of these conditions.</p> <p>Regarding the organization field, the IPT clarifies that the organization field is treated differently based on the requirements listed in the policy recommendation 12. Specifically, as drafted in Section 6.6 and implementation note D of the draft policy language, registrars must receive an agreement from the Registered Name Holder before publishing the data elements listed in the organization field.</p>
-----------------------	--	---

<p>9.2.1</p>	<p>“Paragraph 9.2.1 allows the redaction of non Personal Data contained in the Registration Data if there is a "commercially reasonable," purpose to do so. The fundamental purpose of the specification is to facilitate compliance with applicable privacy law. Whether redaction of non-personal data impacts a Registry Operator or Registrar's commercial business is beyond the scope of the process. More to the point, the use of the broad term "commercially reasonable" without definition undermines the fundamental purpose of a specification by inserting significant ambiguity into the specification.” (BC)</p>	<p>The IPT clarifies that the term "commercially reasonable" is utilized in the draft Registration Data Policy as it is used in the policy recommendations. Since the term's definition is subjective and open to interpretation based on the perspectives and business models of registrars, the IPT refrained from providing a specific definition in the draft policy.</p>
---------------------	---	---

Addendum I

<p>Addendum I</p>	<p>“Web-based lookups are required under the Registrar Accreditation Agreement.” (BC)</p>	<p>The IPT confirms that the web-based lookups are required in the Registrar Accreditation Agreement. Additionally, the IPT clarifies that the RDAP provisions regarding redaction are contained within the RDAP profile and are not excluded in Addendum I and II of the Registration Data Policy.</p>
<p>Addendum I</p>	<p>“It seems this implicitly excludes RDAP(?), which doesn't make sense.” (IPC)</p>	

Addendum II

<p>Addendum II</p>	<p>“As noted in previous comments from many parts of the community, it would be irresponsible to allow Contracted Parties to delete Registrant Organization data. This risks fundamentally and irreparably changing the entity responsible for domain name ownership, which is an unacceptable outcome.” (IPC)</p>	<p>The IPT clarifies that the deletion of the registrant organization data is implemented as described in Recommendation 12 of the EPDP Final Report which was adopted by the Board following consultation with the GNSO Council and supported by the IRT.</p>
---------------------------	---	--

Background

<p>Background</p>	<p>“The final paragraph of the Draft Registration Data Policy should be completed before the Draft becomes Policy.” (Tucows)</p>	<p>The IPT will incorporate the Registration Data Policy publication date within the policy language prior to the draft becoming an ICANN Consensus Policy.</p>
--------------------------	---	---

3.4 Input suggesting Policies and Procedures were Incorrectly Redlined

Input Received		Implementation Project Team Response
<p>AWIP</p>	<p>IPC suggested that the “redlines within the existing AWIP policy are incorrect” but did not elaborate further. (IPC)</p>	<p>Following further review, the IPT clarifies that the published version of the AWIP is based on IRT discussion and approval, however based on comments received the IPT incorporated additional updates to the AWIP for IRT review and discussion.</p>
<p>ERRP</p>	<p>“The recommended changes include dropping the term “Registrant” and replacing with “Registered Name Holder.” This change was not part of the recommendations and this change makes the policy inconsistent with prior policies that refer to “registrant”. This policy should make clear that Registrant and “Registered Name Holder” are synonymous.” (BC)</p>	<p>The IPT clarifies that the updates to the ERRP were made to consistently refer to “Registered Name Holder”, rather than reference both Registered Name Holder and Registrant interchangeably. This is to ensure consistency with the Registration Data Policy, in line with Recommendation 27 and to avoid confusion caused by using different terminology to describe the same person/entity.</p>
<p>IGO & INGO Identifiers</p>	<p>“The recommended changes include dropping the term “Registrant” and “domain name registrant” and replacing with “Registered Name Holder.” This change was not part of the recommendations and this change makes the policy inconsistent with prior policies that refer to “registrant”. This policy should</p>	<p>The IPT clarifies that the redlines to the protection of IGO & INGO were made to consistently refer to “Registered Name Holder”, rather than reference both Registered Name Holder and Registrant interchangeably. This is to ensure consistency with the Registration Data Policy, in line with Recommendation 27 and avoid confusion caused by using different terminology to describe the same person/entity.</p>

	<p>make clear that Registrant, “Domain Name Registrant”, and “Registered Name Holder” are synonymous.” (BC)</p>	
<p>CL&D</p>	<p>“The requirement for maintaining a WHOIS lookup web based service on the contracted parties website’s should not be eliminated. See the BC’s comments to the RDAP implementation posted at https://www.icann.org/en/public-comment/proceeding/proposed-amendments-to-the-base-gtld-raa-and-raa-to-add-rdap-contract-obligations-06-09-2022/submissions/icann-business-constituency-bc-16-11-2022” (BC)</p>	<p>The IPT clarifies that the updates made to the CL&D policy do not eliminate, but alternatively separate, the requirements for a WHOIS lookup web based service. Specifically noting:</p> <ul style="list-style-type: none"> • “Section 1 of this policy details technology-agnostic requirements that apply to all Registration Data Directory Services. • <i>Section 2 of this policy details implementation requirements pertaining to WHOIS (available via port 43) and web-based Whois directory services only.</i>”
<p>Transfer FOA Rr</p>	<p>“The EPDP Phase 1 Policy did not authorize these changes: - The change of “registrant” to “registered name holder.” - The deletion of “ in the event of a dispute the Registered Name Holder’s authority supersedes the administrative contact’s authority” - Footnote 1 which incorrectly attempts to define “Registered Name Holder” This definition is inconsistent with RAA Section 1.16 where it states that "Registered Name Holder" means the holder of a Registered Name. The IRT did not have authority to redefine definitions in the RAA. - Elimination of the “Transfer Contact” throughout. - Elimination of the Form of Authorization. Indeed they create security risks since Forms of Authorizations (FOA) were intended to make transfers more secure by preventing domain name hijacking. When DPAs are implemented and more contact information is available (such as when NIS2 requirements apply to the data of legal persons and/or natural person registrants consent to the publication of their information), the FOAs should be required rather than eliminated. - Addition of the “where required pursuant to Section I.A.2.” throughout, such as in Section 2.2.1., 2.2.4, 4.1, 4.3 - Registrant Transfers- Deletion of 1.1.4 in Section II.A. Instead - technical contact should be substituted for the administrative contact. These changes are not necessary to implement the Phase 1 Policy and should be deleted. In addition, more work is needed to determine whether it would be more appropriate to substitute the “technical contact” for the “administrative contact” in the transfer policy since there may be</p>	<p>The IPT would like to clarify that the updates to the Transfer FOA Confirmation are consistent with the requirements specified in EPDP Phase 1 policy recommendations and do not aim to redefine terms or eliminate requirements. Specifically, Recommendation 27 requires updates to policies and procedures that refer to data elements no longer required by the EPDP Phase 1 policy recommendations, such as administrative and/or technical contact. The Registration Data Policy eliminates the administrative contact, eliminating the Transfer Contact as defined/described in the Transfer Policy. As the only remaining authorized contact is the RNH, the term “registrant” was eliminated to avoid confusion and duplication of definitions. Furthermore, the FOA requirements are not eliminated through the updates but rather references the Board deferral of compliance enforcement of the Gaining FOA requirement. Lastly, the IPT encourages the BC to actively participate in the ongoing Transfer PDP WG deliberations to consider further concerns regarding the technical and administrative contact within the Transfer policy.</p>

	<p>instances where the technical contact may be more closely aligned with what was formerly the administrative contact. Indeed, this creates a security risk when there are multiple contacts (registrant and tech contact), and the registrant is unresponsive or goes out of business. Examples of where this might arise could be situations where the reseller or privacy/ proxy service is the registrant, and the technical contact is the customer of the reseller, privacy/proxy service. This is especially important when more registrations reflect registrant information that apply to resellers or privacy/proxy providers. Instead, the policy should replace “administrative contact” with “technical contact” to have an additional way of enabling the transfer.” (BC)</p>	
<p>Transfer FOA initial auth.</p>	<p>“The EPDP Phase 1 Report did not authorize these changes: - The elimination of a second form of authorization in the FOA. As a result, the policy should reflect “technical contact” in lieu of “administrative contact” throughout. - The elimination of a reference to a “WHOIS database”. The changes assume that there are no contacts in the RDS database that are public, yet ICANN policy clearly requires contacts to be published when the registrant consents, and there may be legal requirements such as NIS2 where the data of legal persons is required to be published. These changes are not necessary to implement the Phase 1 Policy and should be deleted.” (BC)</p>	<p>As previously noted, the updates to the Transfer FOA initial authorization and TDRP were carefully reviewed and remain consistent with requirements specified in EPDP Phase 1 policy recommendations. The updates eliminate the FOA requirements and only reference the Board deferral of compliance enforcement of the Gaining FOA requirement. Additionally, the IPT notes that the public WHOIS database does not define the RNH, therefore the entity to whom the FOA should be sent should not be defined in the public database. Finally, the IPT is unable to substitute the technical contact for the administrative contact as it is not part of the EPDP Phase 1 policy recommendations.</p>
<p>TDRP</p>	<p>“The EPDP Phase 1 Policy did not authorize these changes: - The change of “registrant” to “registered name holder.” - Elimination of the “Transfer Contact” throughout. - Elimination of the Form of Authorization. Indeed they create security risks since Forms of Authorizations (FOA) were intended to make transfers more secure by preventing domain name hijacking. When DPAs are implemented and more contact information is available (such as when NIS2 requirements apply to the data of legal persons and/or natural person registrants consent to the publication of their information), the FOAs should be required rather than eliminated. - The deletion of a duplicate form of authorization - instead of eliminating the</p>	

	<p>“administrative contact “ throughout, it should be replaced with the technical contact. These changes are not necessary to implement the Phase 1 Policy and should be deleted. See above for explanation for why these changes are inappropriate.” (BC)</p>	
<p>Transfer Policy</p>	<p>“The EPDP Phase 1 Policy did not authorize these changes: - The change of “registrant” to “registered name holder.” - The deletion of “ in the event of a dispute the Registered Name Holder’s authority supersedes the administrative contact’s authority” - Footnote 1 which incorrectly attempts to define “Registered Name Holder” This definition is inconsistent with RAA Section 1.16 where it states that "Registered Name Holder" means the holder of a Registered Name. The IRT did not have authority to redefine definitions in the RAA. - Elimination of the “Transfer Contact” throughout. - The requirement of a “secure method of transfer” in Section 2.2.1 before any registration data can be transferred. No secure method of transfer is needed for information that is publicly available. When DPAs are implemented and more contact information is available (such as when NIS2 requirements apply to the data of legal persons and/or natural person registrants consent to the publication of their information), this information can be shared without further restrictions as imposed by proposed implementation.</p> <p>- Elimination of the Form of Authorization. Indeed they create security risks since Forms of Authorizations (FOA) were intended to make transfers more secure by preventing domain name hijacking. When DPAs are implemented and more contact information is available (such as when NIS2 requirements apply to the data of legal persons and/or natural person registrants consent to the publication of their information), the FOAs should be required rather than eliminated. - Addition of the “where required pursuant to Section I.A.2.” throughout, such as in Section 2.2.1., 2.2.4, 4.1, 4.3 - Registrant Transfers- Deletion of 1.1.4 in Section II.A. Instead - technical contact should be substituted for the administrative contact.- The language regarding “best practices” for generating AuthCodes should be strengthened to require the generation of</p>	<p>The updates to the Transfer Policy were carefully reviewed and remain consistent with requirements specified in EPDP Phase 1 policy recommendations. The updates do not redefine terms or eliminate requirements, but rather update impacted policies and procedures as recommended by Recommendation 27. As a result, the administrative and transfer contacts were eliminated, making the remaining authorized contact the RNH. The IPT incorporated these updates to avoid confusion and duplication of definitions. Regarding the FOA, the IPT clarifies that requirements were not eliminated through the redlines and only reference the Board deferral of compliance enforcement of the Gaining FOA requirement. The IPT notes that the public WHOIS database does not define the RNH, so the entity to whom the FOA should be sent should not be defined in the public database. Finally, the IPT notes that the AuthInfo code must be provided to the RNH per Section 5.2 of the Transfer Policy. The IPT encourages the BC to provide any further feedback or concerns to the chair of the RDAP working group.</p>

	<p>AuthCodes, with the “best practices” to apply to how they are transmitted. These changes are not necessary to implement the Phase 1 Policy and should be deleted.</p> <p>In addition, more work is needed to determine whether it would be more appropriate to substitute the “technical contact” for the “administrative contact” in the transfer policy since there may be instances where the technical contact may be more closely aligned with what was formerly the administrative contact. Indeed, this creates a security risk when there are multiple contacts (registrant and tech contact), and the registrant is unresponsive or goes out of business. Examples of where this might arise could be situations where the reseller or privacy/ proxy service is the registrant, and the technical contact is the customer of the reseller, privacy/proxy service. This is especially important when more registrations reflect registrant information that apply to resellers or privacy/proxy providers. Instead, the policy should replace “administrative contact” with “technical contact” to have an additional way of enabling the transfer.” (BC)</p>	
<p>UDRP Policy</p>	<p>“The EPDP Phase 1 Report did not authorize these changes: - The elimination of a reference to a “WHOIS database”. The changes assume that there are no contacts in the RDS database that are public, yet ICANN policy clearly requires contacts to be published when the registrant consents, and there may be legal requirements such as NIS2 where the data of legal persons is required to be published. - Footnote 1 should be deleted since there is no reason to replace “WHOIS database” with Registration Data. These changes are not necessary to implement the Phase 1 Policy and should be deleted.” (BC)</p>	<p>The IPT clarifies that reference to “WHOIS database” was removed to ensure the UDRP policy remains technology agnostic.</p>
<p>UDRP Rules</p>	<p>“The EPDP Phase 1 Report did not authorize these changes: - The elimination of a reference to a “WHOIS database”. The changes assume that there are no contacts in the RDS database that are public, yet ICANN policy clearly requires contacts to be published</p>	<p>The IPT clarifies that reference to “WHOIS database” was removed to ensure the UDRP Rules policy remains technology-agnostic. Regarding the addition of <i>“Registration Data Directory Service (hereinafter “RDDS”)</i>”, the IPT notes Registration Data is defined in the draft policy and was incorporated into the UDRP rules based on the capitalized</p>

	<p>when the registrant consents, and there may be legal requirements such as NIS2 where the data of legal persons is required to be published. - Footnote 1 should be deleted since there is no reason to replace “WHOIS database” with Registration Data. - In Section 2(a)(2) - the insertion of <i>“Registration Data Directory Service (hereinafter “RDDS”) or in the Registration Data provided by the Registrar or Registry Operator when the Registration Data is redacted in the RDDS”</i> is not needed. When there is a Redacted Contact in the public RDDS queries, the unredacted RDDS would still be available to be provided under the Rules. This change implies that the Registrar can list other data (such as customer data) beyond the unredacted information - which is clearly not possible. These changes are not necessary to implement the Phase 1 Policy and should be deleted.” (BC)</p>	<p>definition of “Registration Data Policy” which concerns data elements collected or generated in conjunction with Section 6 of the draft policy.</p>
<p>URS Rules</p>	<p>“Section 4 should replace the new ‘Registration Data’ with ‘RDDS’” (BC)</p>	<p>The IPT kindly refers to section 3.6 of the draft Registration Data Policy which defines the use of “Registration Data” as data elements that are generated or collected. Additionally, Section 4 of the URS Rules considers the country or territory of both Registration Data or RDDS to be the same due to the identical publication requirements for the data elements.</p>
<p>WDRP Rules</p>	<p>The EPDP Phase 1 Policy did not authorize these changes: - The change of “registrant” to “registered name holder” throughout. - In the first paragraph the replacement of “Registration Data” is incorrect since Registration Data includes information that is not generated by the Registrant.</p> <p>- The deletion of the requirement to send the notice to a duplicate contact - instead of eliminating the “administrative contact” throughout, it should be replaced with the technical contact. More work is needed to determine whether it would be more appropriate to substitute the “technical contact” for the “administrative contact” in the WHOIS Data Reminder Policy since there may be instances where the technical contact may be more closely aligned with what was formerly the administrative contact. Indeed, this creates a security risk when there are multiple contacts (registrant and tech contact), and the registrant is unresponsive or</p>	<p>The IPT clarifies that Registration Data includes generated items such as creation date and expiration date and is not limited to data collected from the RNH. The draft Registration Data Policy eliminates the administrative and transfer contacts, subsequently making the authorized contact the RNH. The IPT incorporated these updates as required in Recommendation 27 to mitigate against confusion and duplication of definitions. Lastly, the term “WHOIS data” was replaced as WHOIS data includes information that is collected or generated.</p>

	<p>goes out of business. Examples of where this might arise could be situations where the reseller or privacy/ proxy service is the registrant, and the technical contact is the customer of the reseller, privacy/proxy service. This is especially important when more registrations reflect registrant information that apply to resellers or privacy/proxy providers. Instead, the policy should replace “administrative contact” with “technical contact” to have an additional way of ensuring that the information provided is accurate.” (BC)</p>	
<p>RDAP Guide</p>	<p>“As stated above the BC believes that Web-based lookups must continue to be required under the Registrar Accreditation Agreement. An obligation to only respond to RDAP queries using a non-human readable/parsable network protocol is insufficient to ensure Internet users have access to Registration Data as required by the ICANN bylaws.” (BC)</p>	<p>The IPT clarifies that web based lookup requirements were not eliminated and the draft RDAP guide is written to ensure the draft policy remains technology-agnostic. The IPT encourages the BC to review the Public Comment Summary Report for the Proposed Amendments to the Base gTLD RA and RAA to Add RDAP Contract Obligations for further clarification.</p>
<p>RDAP Profile</p>	<p>“As stated above the BC believes that Web-based lookups must continue to be required under the Registrar Accreditation Agreement. An obligation to only respond to RDAP queries using a non-human readable/parsable network protocol is insufficient to ensure Internet users have access to Registration Data as required by the ICANN bylaws. Attachment: BC Comment on Draft policy for gTLD Registration data.pdf (209.17 KB) Summary of Attachment: The attached PDF is in lieu of completing this form, since the attachment includes formatting that should assist readers in identifying line breaks, lists, text excerpts, strike-throughs, etc. Summary of Submission: The final NIS2 text was adopted by the European Parliament on 10-Nov-2022. The BC and other members of the EPDP frequently cited pending NIS2 regulation in our advice to create evolution mechanisms for registrant data policy. Unfortunately, the EPDP Working Group and GNSO Council did not follow that advice. NIS2 now requires EU Member States to enact regulation that may render some EPDP policy recommendations in conflict with law. Specifically, NIS2 requirements to publish registrant data for legal persons, requirements to maintain</p>	

accurate registrant data, and potentially requirements for registries to maintain registrant data (i.e. Thick Whois). The BC therefore recommends that implementation of EPDP Phase 1 and Phase 2 be reassessed after the first EU Member State implements regulations pursuant to NIS2.” (BC)

3.5 General Comments

Input Received

Implementation Project Team Response

2 & 10

“In Section 10, the recommendations are indefinite as to the responsibilities of the contracted parties in evaluating requests for access to information. Further, the recommended response times are unduly long and burdensome on the requestor who endeavors to act quickly on suspected cases of abuse. INTA requests that the drafters of the policy reconsider these sections based on INTA's specific observations so that the system will be consistent, predictable and more user friendly.” (INTA)

The IPT clarifies that the scope of the Registration Data Policy is strictly limited to processes and does not provide criteria or requirements on how contracted parties determine whether to disclose data or not. Additionally, the IPT confirms that the draft policy language was implemented in line with [Recommendation 18](#) which requires “Response time for a response to the requestor will occur without undue delay, but within maximum of 30 days”.

“We welcome the work of ICANN to release the document in line with [Workstream 2 Recommendations on ICANN Transparency](#). Our analysis shows that, primarily, the document is a good first step **but has fundamental gaps in ensuring the full implementation of Section 27.2 of the ICANN Bylaws (on Human Rights) and other Bylaws with an impact on human rights**. CCWP-HR, therefore, urges ICANN to implement the recommendations below, which would ensure that the Draft Registration Data Policy is implemented more closely with international law and best practice.”

Comments on the lack of clear timelines

The draft policy states that the effective date of the policy shall be “no later than [540 days after the date of policy announcement and legal notice for implementation]”. However, the call for Public Comment that accompanies the draft Policy states: “**after the implementation plan has been finalized, ICANN's Contracted Parties will be notified of the implementation and compliance deadlines.**” We recommend that the language in both documents be changed to either specify an exact date or ensure that the language is consistent, so that all stakeholders have clarity and legal certainty. Given that the draft policy aims to further enhance the privacy of registrants, we recommend that the deadline for compliance be made as soon as practicable (preferably within the first 6 months), as any further delay in securing the rights to privacy of registrants puts their data at risk.”

Comments on the requirements for Data Protection Agreements

We welcome the requirement that “ICANN, gTLD Registry Operators, and accredited Registrars MUST enter into required data protection agreements with each other and with relevant third party providers contemplated under this Policy where applicable law requires. The terms may include legal bases for processing Registration Data.”

We recommend that the requirement be made more robust to additionally include mandates on ICANN, gTLD registry operators and accredited registrars to conduct full human rights impact

Input regarding the lack of clear timelines

The IPT clarifies that the effective date will be published after finalization of policy language, and an exact publication date cannot be determined until all comments have been considered that could impact policy requirements. Thus, until this Policy’s effective date, the requirements in the Temporary Specification for gTLD Registration Data, applicable via the Interim Registration Data Policy, will continue to apply. The IPT further clarifies that the Temporary Specification [was adopted by the ICANN Board to provide](#) “modifications to existing requirements in the Registrar Accreditation and Registry Agreements to bring them into compliance with the European Union’s General Data Protection Regulation (GDPR).”

Input on the Requirements for Data Protection Agreements

The IPT notes the comment that the requirement should be “made more robust to additionally include mandates on ICANN, gTLD registry operators and accredited registrars to conduct full human rights impact assessments (HRIAs) or data protection impact assessments (DPIAs), carried out by independent experts, within one year after the compliance deadline and at least every two years thereafter.” Because the EPDP Phase 1 team did not recommend the incorporation of such requirements in this Policy, this suggestion is beyond the scope of this implementation.

Input regarding the Collection of Registration Data

The IPT notes that the EPDP Phase 1 team did not recommend the incorporation of the suggested requirements in this policy, thus the recommendation to obtain “express” consent from the registrant prior to collection and informing registrants of what data is or is not required within this policy is beyond the scope of this implementation. The IPT would also like to note that section 3.7 of the [Registrar Accreditation Agreement](#) already requires the Registrar to obtain consent from the registrant and inform them of which data is required.

Input regarding the deletion of the Admin contact

The IPT notes that the recommendation to make the deletion of the administrative contact mandatory is beyond the scope of this implementation as the EPDP Phase 1 team did not include this requirement in this Policy. However the IPT references implementation note A of this Policy, which “does not prohibit Registries or Registrars from processing data for purposes beyond the scope of this policy.”

Input regarding Disclosure Requests Independent mechanism

assessments (HRIAs) or data protection impact assessments (DPIAs), carried out by independent experts, within one year after the compliance deadline and at least every two years thereafter. HRIAs and DPIAs are activities that include engaging in consultation with both internal and external stakeholders of an entity. This is done so that the entity can accurately determine the potential and actual effects of their corporate policies, practices, products, and services on human rights and data protection, respectively, and then take steps to lessen the effects of any adverse effects. The HRIA has been acknowledged by ICANN itself as a methodology through which it can comply with its commitments as outlined in Section 27.2 of the ICANN Bylaws (on human rights) as well as in the Framework Of Interpretation for Human Rights (FOI-HR). Under the United Nations Guiding Principles (UNGPs) on Business and Human Rights, companies including ICANN, gTLD registry operators and accredited registrars are responsible for respecting the human rights of their stakeholders and customers. Conducting HRIAs and DPIAs will ensure that these companies are not only in compliance with international human rights standards and principles, but also with their national and regional obligations, such as those under the European Union General Data Protection Regulations (GDPR).

Comments on the requirements for Collection of Registration Data

Under **Section 6.7 and the Implementation Notes of the draft policy, there is leeway for gTLD registry operators, and accredited registrars to a) collect data in addition to the data provided for under the draft policy and b) process data for purposes that are beyond the scope of this draft policy.** We recommend that these sections be redrafted to require ICANN registries and gTLD registry operators to a) obtain the express consent of Registrants before the collection of data and b) clearly inform registrants of what data is required and not required to be collected under this draft policy, prior to obtaining registrant consent to collection.

Comments on the requirements for deletion of administrative contact data

The IPT clarifies that during the policy development phase, the EPDP Phase 1 team recommended a timeline and criteria for registrars' and registry operators' response to requests for data access, but did not recommend any specific processes the contracted parties must follow in evaluating a request for access and, if applicable, disclosing the requested data (which might, or might not, include notification of the registrant). As such, this issue is beyond the scope of the EPDP Phase 1 policy, though the contracted parties may have additional requirements in this area pursuant to local law. Please note that this issue was considered in greater depth by the EPDP Phase 2 team.

We welcome the recommendation, which allows gTLD registry operators and accredited registrars to **delete administrative contact data** that was collected prior to the publication of the draft Data Consensus Policy but note that the **drafting makes it optional by the use of “MAY” instead of “MUST”**. **We therefore recommend that this be redrafted to make it mandatory, unless the express, informed consent of the Registrant is provided or in the case of ongoing law enforcement processes at the time of the policy's publication**

Comments on Disclosure Requests.

We welcome this section, as it requires that, when providing responses to disclosure requests, gTLD registry operators and accredited registrars' responses must provide an explanation of how the fundamental rights and freedoms of the data subject were weighed against the legitimate interest of the requestor (if applicable). **However, this provision applies as a response to a third-party requester for data and does not clearly allow for the involvement of registrants in decisions involving their data. The lack of provisions for notifying registrants when requests to access their registration data are made undermines their ability to challenge these requests. As such, this mechanism does not adequately balance the needs of a third-party requester for access to information with registrants' rights to privacy and data protection. To ensure compliance with the principles of necessity, proportionality, and the requirement for due process under the international human rights framework, we advise that users and registrants be provided with an independent mechanism to appeal requests before their registration data is disclosed to third-party requesters.” (CCWP-HR)**