Comment of the ICANN Business Constituency (BC)

Data Processing Specifications (DPS) for the RAA and RyA

9-Sep-2024

The Business Constituency (BC) welcomes the opportunity to provide feedback on the draft Data Processing Specifications (DPS) for the Registrar Accreditation Agreement (RAA) and the Registry Agreement (RyA).

We acknowledge the critical importance of data protection and appreciate ICANN's efforts to ensure compliance with global data privacy regulations, particularly in the context of the General Data Protection Regulation (GDPR). The BC recognizes the complex challenges involved in balancing privacy with the need for access to gTLD registration data, and we commend the collaborative efforts of ICANN and the Contracted Party House in developing these draft specifications.

Importance of Data Protection

Data protection is a fundamental principle that underpins trust in the digital economy. The BC fully supports ICANN's commitment to safeguarding personal data and ensuring that processing of registration data complies with applicable laws. We recognize these efforts are essential for legal compliance and for maintaining the integrity and stability of the global domain name system (DNS).

Specific Concerns

While the BC supports the overarching goals of the DPS, we would like to highlight several concerns that are critical to our members:

1. **Data Access**: The BC is particularly concerned about how the DPS might impact access to registration data for legitimate purposes, such as cybersecurity, intellectual property protection, and law enforcement. We urge ICANN to ensure that the DPS includes clear and consistent guidelines for access to data, balancing privacy considerations with the need for transparency and security.

Audits & Research: We note that the DPS does not include obligations to transfer all data requested by ICANN for the purposes of conducting audits of the contracted parties under the applicable contracts or consensus policies. In addition, the DPS does not obligate the contracted

parties to transfer all data requested by ICANN to conduct research or surveys in support of its consensus policy processes, such as the accuracy studies that have recently been put on hold.

Privacy and Proxy Services: A related concern involves the role of Privacy and Proxy (P/P) services in the context of data access. Even if a registrar approves a legitimate request for registration data, the effectiveness of this access is nullified if the relevant data is obscured by a P/P service that is not contractually obligated to honor the registrar's determination. For businesses, this creates a significant barrier to protecting intellectual property, enforcing security measures, and responding to legal inquiries. We recommend that ICANN include specific obligations for P/P services within the DPS to ensure that they support the registrar's decisions, thereby maintaining a balance between privacy and the legitimate needs of businesses for data transparency.

Thick WHOIS: The DPS must also create the necessary **transfers** to enable Thick Whois under ICANN's recently adopted consensus policy. See Section 7.4 of the new Registration Data Policy:

> *7.4. Registrar MUST transfer the following data elements to Registry Operator, if collected, provided an appropriate legal basis exists and data processing agreement is in place:*
>
> *7.4.1. Registrant Organization*
>
> *7.4.2. Registrant State/Province*
>
> *7.4.3. Registrant Postal Code*
>
> *7.4.4. Registrant Phone Ext*
>
> *7.4.5. Registrant Fax*
>
> *7.4.6. Registrant Fax Ext*
>
> *7.4.7. Tech Name*
>
> *7.4.8. Tech Phone*
>
> *7.4.9. Tech Email*

Since the DPS will serve as the Data Processing Agreement for this policy, it needs to ensure that each of these data elements will be **transferred** to the applicable registry from the registrar in accordance with the applicable consensus policy.

Compliance with Law: The DPS should also enable the transfer and processing of registrant data in order to comply with applicable law or for data transfers allowed under GDPR such as under Article 49 (1) (e) when they are "necessary for the establishment, exercise, or defense of legal claims."

For example, the EU Directive on Network and Information Systems (NIS2), which must be transposed into member state law by October 2024, includes requirements to collect, maintain,

and verify registrant information that apply to registries, registrars, and other entities providing domain name registration services, such as privacy/proxy providers and resellers.

As a result, an additional purpose should be added (2.1.10) to comply with the requirements of applicable law to collect, maintain, process, verify, disclose, transfer, and publish any registration data (including the data of the beneficial user or customer of a privacy or proxy service) that is specified under applicable law. Also, Section 2.1.3 should be updated to add " or in accordance with applicable law, such as NIS2" at the end thereof. This obligation to comply with NIS2 (as applicable) should recognize that the parties to the DPS may transfer and enable the processing of data by service providers for specific requirements under NIS2, such as to verify or audit the accuracy of the contact data.

Managing the RDRS: Currently, there is no mention of the transfer of personal data to ICANN regarding the management and operation of the Registration Directory Registration System (RDRS). Yet ICANN is unable to access the personal data to resolve complaints or issues related to the RDRS (which is not a consensus policy, but a pilot system). Ensuring that ICANN is able to access this information to be able to respond to complaints or operational issues even if the system is a voluntary one should be separately addressed in the DPS.

Considerations for Service Providers - Section 4 addresses the processing of registration data among the contracted parties and ICANN to comply with privacy laws, but does not address situations where transfers are to take place for reasons as allowed under the DPA. For example, data may be transferred to service providers used by ICANN to conduct its security operations, research, or conduct surveys. As a result, Sections 4.3 - 4.5 should be modified to reference the purposes allowed under the Agreement, the DPS, and to comply with applicable laws, including NIS2.

Data Subject Rights - Section 7 should include a new Section 7.5 that tracks the accuracy obligations of GDPR under Article 5(d) that personal data be "accurate, and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay."

1. Compliance Costs: The implementation of the DPS may result in increased costs for contracted parties, including registrars and registries. These costs could ultimately be passed on to businesses and consumers. The BC requests that ICANN carefully assess whether the proposed DPS imposes undue financial burdens on contracted parties and consider ways to mitigate these costs.

2. Transparency and Accountability: The BC emphasizes the need for transparency in how gTLD registration data is processed under the DPS. We encourage ICANN to establish robust accountability mechanisms to ensure that all parties involved adhere to the

agreed-upon data processing standards. This includes regular reporting and audits to verify compliance.

3. Flexibility: The rapidly evolving nature of data protection laws worldwide necessitates a degree of flexibility in the DPS. The BC suggests that ICANN consider incorporating provisions that allow for adjustments to the DPS without requiring extensive renegotiations, ensuring that the specifications remain relevant and compliant with future legal developments. These could include changes to consensus policies and future requirements, such as those imposed by member states as they transpose NIS2.

4. **Definitions.**

   Section 1.1 "Applicable Laws" should specifically include NIS2 since it directly affects the applicability of GDPR.

   Section 1.6 "Personal Data" should remove "or legal person".

   Section 1.10 "Service Provider" should specifically include third parties that are mentioned in the Agreements, such as privacy/proxy providers, resellers, and escrow agents, all of which are required to collect, transfer, process, and disclose data.

Strategic Insights

To better support the business community while protecting personal data, the BC suggests the following improvements:

1. Enhanced Access Mechanisms: ICANN should explore the possibility of implementing tiered access mechanisms that allow different levels of data access based on the requester's purpose and legal standing. This approach would help balance the need for privacy with the legitimate needs of various stakeholders, including businesses that rely on registration data for security and enforcement purposes.

2. Cost Mitigation Strategies: ICANN should consider developing cost mitigation strategies for the implementation of the DPS. This could include financial support for smaller registrars or tiered compliance requirements based on the size of the business, ensuring that smaller entities can comply without undue financial burden on contracted parties.

3. Increased Stakeholder Engagement: The BC recommends ongoing engagement with all stakeholders, including the business community, to refine and improve the DPS. Regular consultations will help ensure that the DPS continues to meet the diverse needs of the ICANN community while remaining compliant with global data protection standards.

Additional Safeguards

To align the DPS with the BC's priorities, we suggest the following additional safeguards:

1. Regular Review and Update Mechanism: The DPS should include a mechanism for regular review and updates to ensure it remains aligned with evolving data protection laws and the needs of the ICANN community.

2. Clear Definitions and Scope: The DPS should provide clear definitions of key terms and the scope of data processing activities. This will reduce ambiguity and ensure consistent interpretation and application across all parties.

3. Dispute Resolution Process: The BC advocates for the inclusion of a clear and efficient dispute resolution process within the DPS. This will provide a structured approach for addressing disagreements between contracted parties and ICANN regarding data processing practices.

Conclusion

The BC appreciates the opportunity to provide feedback on the draft DPS and looks forward to continued collaboration with ICANN to ensure that the final specifications reflect the needs of the business community while upholding the highest standards of data protection. We believe that with the suggested improvements and safeguards, the DPS can achieve a balanced approach that protects personal data, interests of all stakeholders while maintaining the integrity and functionality of the global DNS.

This comment was drafted by Segunfunmi Olajide, Margie Milam, and Steve Crocker.
It was approved in accord with the BC Charter.