Work on the topic of Standardized Access to Non-Public Registration data shall begin once gating questions (purposes, collection of registration data by registrar, transfer of data from registrar to registry, publication of data by registrar / registry) have been answered and finalized in preparation for the Temporary Specification Initial Report. The threshold for establishing "answered" for the gating questions shall be consensus of the EPDP Team and non-objection by the GNSO Council.

Following the EPDP Team's primary focus on confirming, amending, rejecting or replacing the Temporary Specification, and resolving the gating questions identified above, the EPDP Team shall turn its attention to the items included in the Temporary Specification Annex, listed as "Important Issues for Further Community Action." These include but are not limited to the standardized access model referenced above.

Phase II: System for Standardized Access to Non-Public Registration Data and Annex - Important Issues for Community Consideration

System for Standardized Access to Non-Public Registration Data

a) Purposes for Accessing Data - what are the unanswered policy questions that will guide implementation?

- a1) Under applicable law, what are legitimate purposes for third parties to access registration data?
- a2) What legal bases exist to support this access?
- a3) What are the eligibility criteria for access to non-public Registration data?
- a4) Do those parties/groups consist of different types of third-party requestors?
- a5) What data elements should each user/party have access to based on their purpose?
- a6) To what extent can we determine a set of data elements and potential scope (volume) for specific third parties and/or purposes?
- a7) How can RDAP, that is technically capable, allow Registries/Registrars to accept accreditation tokens and purpose for the query? Once accreditation models are developed by the appropriate accreditors and approved by the relevant legal authorities, how can we ensure that RDAP is technically capable and is ready to accept, log and respond to the accredited requestor's token?

b) Credentialing - What are the unanswered policy questions that will guide implementation?

- b1) How will credentials be granted and managed?
- b2) Who is responsible for providing credentials?
- b3) How will these credentials be integrated into registrars'/registries' technical systems?

c) Terms of access and compliance with terms of use - What are the unanswered policy questions that will guide implementation?

- c1) What rules/policies will govern users' access to the data?
- c2) What rules/policies will govern users' use of the data once accessed?
- c3) Who will be responsible for establishing and enforcing these rules/policies?
- c4) What, if any, sanctions or penalties will a user face for abusing the data, including future restrictions on access or compensation to data subjects whose data has been abused in addition to any sanctions already provided in applicable law?
- c5) What kinds of insights will Contracted Parties have into what data is accessed and how it is used?
- c6) What rights do data subjects have in ascertaining when and how their data is accessed and used?
- c7) How can a third party access model accommodate differing requirements for data subject notification of data disclosure?

Annex: Important Issues for Further Community Action

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

2 Addressing the feasibility of requiring unique contacts to have a uniform anonymized email address across domain name registrations at a given Registrar, while ensuring security/stability and meeting the requirements of Section 2.5.1 of Appendix A.

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

4 Consistent process for continued access to Registration Data, including non-public data, for users with a legitimate purpose, until the time when a final accreditation and access mechanism is fully operational, on a mandatory basis for all contracted parties.

5 Distinguishing between legal and natural persons to allow for public access to the Registration Data of legal persons, which are not in the remit of the GDPR.

6 Limitations in terms of query volume envisaged under an accreditation program balanced against realistic investigatory cross-referencing needs.

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