Dear Councilors,

I am including a summary of my recent meeting with the ICANN Org SSAD ODP colleagues on 20 October.

The SSAD ODP Team identified additional questions and assumptions, which we discussed during our meeting. The assumptions and my responses are annexed to this message for your information. The SSAD ODP Team plans, pending no objection from the GNSO Council, to proceed with its work on the basis of these assumptions and my responses thereto. The verified assumptions will be used by the SSAD ODP Team as it continues to work on an assessment to inform the Board's review of the EPDP Phase 2 SSAD-related policy recommendations.

Lastly, we briefly discussed the upcoming SSAD ODP Project Update #3 and Community Discussion Webinar, which will take place during ICANN72 on Thursday, 28 October at 19:30 UTC. The SSAD ODP Team recognizes that this session conflicts with the GNSO Council Wrap-Up; however, if any councilors have additional questions not addressed during the session, I am happy to bring these to the attention of the SSAP ODP Team during our next meeting in November.

Please let me know if you have any questions or concerns regarding my responses to the SSAD ODP Team.

Thank you.

Best regards,
JK

The areas identified in the SSAD that interact with ICANN Contractual Compliance, like requestor/data subject procedural complaints and Contracted Party SLA issues, appear to integrate well within the existing processes that ICANN Contractual Compliance employs. For instance, the complaints from requestors and data subjects could come through external facing complaint forms that would be developed, and if needed, automated processes may be developed for processing issues such as those related to SLA violations. From there, the complaints can be processed per ICANN Contractual Compliance's standard approach and processes. *Question 1: Does the proposed approach regarding development of potential complaint forms or automated notifications (where possible) fulfill the intentions of the recommendations?*		Indeed, it was intention – to use the existing ICANN compliance mechanism in case the requestors or registries/registrars could file a compliance complaint in situations prescribed by the policy recommendations. It was never planned, though, that data subjects would use ICANN's compliance mechanism in SSAD context.

Automation of Disclosure Request Processing Per recommendation 9.4, only the following categories are considered to meet the criteria for automated processing of data disclosure: · Requests from Law Enforcement in local or otherwise applicable jurisdictions with either 1) a confirmed GDPR 6(1)e lawful basis or 2) processing is to be carried out under a GDPR, Article 2 exemption; · The investigation of an infringement of the data protection legislation allegedly committed by ICANN/Contracted Parties affecting the registrant; · Request for city field only, to evaluate whether to pursue a claim or for statistical purposes; · No personal data on registration record that has been previously disclosed by the Contracted Party. *Question 2: We note the first bullet specifically references the GDPR. Our understanding is the above categories were included in the legal guidance provided to the EPDP Team, and the legal guidance specifically referenced the GDPR. Our assumption is the EPDP Team considered this guidance in developing this recommendation but did not intend to exclude privacy laws outside the GDPR. In other words, though this first use case only references the specific scenario in which a law enforcement requestor has a legal basis for processing under GDPR 6(1)e (or whose processing is explicitly exempted from GDPR's restrictions on data processing), other law enforcement authorities who are outside the EU might also qualify for automated disclosure if they have a comparable legitimate interest in processing such data under their own local law. Can you please confirm if this assumption is correct (or*		The assumption is correct. Even EPDP was created to develop ICANN policy to accommodate the GDPR requirements, the EPDP Team took broader approach and attempted to formulate recommendations that would correspond not only to the GDPR, but also to all existing and possible future privacy regulations in different parts of the world. Reference to specific provisions of GDPR in 9.4.1 is evident as it was existing regulation at the time of the formulation of the recommendation.

if, conversely, the intention was only for EU law enforcement requests to have the potential for automation under this use case)? *If the above assumption is correct, we also note the recommendation provides for the automation of the use cases described in 9.4.1 - 9.4.4 "from the time of the launch of the SSAD". The SSAD ODP Team will ensure the Operational Design Assessment will include the automation of the specified use cases from Day 1; however, we will note that other use cases outside of the GDPR may be added in future, provided the appropriate processes are followed.*		