All,

We write today with a simple proposal: let's agree to move forward with a hybrid SSAD model as quickly as possible.

By now we are all aware of the Belgian Data Protection Authority's response to ICANN's Unified Access Model for gTLD Registration Data. The CPH has supported ICANN's efforts to gain certainty about the allocation of liability under a centralized system, and we acknowledge the potential benefits of a system in which legal liability for disclosure of gTLD registration data could be removed from us and shifted to a centralized decision-maker. We also note that this is the preferred option for many potential users of SSAD.

ICANN has been clear that diminishing liability for contracted parties is a prerequisite for implementing a centralized model.[1] However, based on the Belgian DPA response, we must accept that specific assurances regarding liability are not coming from the EDPB or the Belgian DPA.

As the Belgian DPA notes, "[i]t is not the role of supervisory authority to validate or approve the suitability of organizational or technical measures which are being considered by a controller as part of its compliance obligations."[2] We cannot rely on data protection authorities to provide definitive answers to these questions. What we can do, however, is rely on the significant amount of guidance and legal advice that this group has collected over nearly two years of examining these issues.

Our findings over this time are consistent and clear: no legal opinion, guidance, or advice received to date suggests that the type of liability shifting required under the centralized model is legally possible. We know from Bird & Bird that liability attaches to the controllers of data, and under a centralized SSAD "the most likely outcome – and certainly most supervisory authorities' starting position – is that CPs are controllers – and, given ICANN's role in determining purposes and means of processing, that they will be joint controllers with ICANN org in respect of their disclosure of Registration Data to Requesters via a SSAD."[3]

Moreover, we cannot deem or disclaim the controller role, as parties "are not free to simply 'designate' which party shall be deemed to act as controller or joint controller[.]"[4] As a result, "each

[1] "And so that means that in essence to have any unified access model whatsoever you either reach an agreement with 2500 contracted parties about what they think is the legal risk they have or you come up with a motions [sic] where you diminish the legal responsibilities for the contracted parties." Goran Marby, EPDP F2F Meeting Transcript, 25 September 2018, pg. 2, available here.

[2] Data Protection Authority (Belgium), Letter to Goran Marby, 4 December 2019, pg. 2, available here.

[3] Phil Bradley-Schmieg & Ruth Boardman (Bird & Bird LLP), "Questions 1&2: Liability, Safeguards, Controller & Processor", 9 September 2019, p.6, 2.18; *see also* Article 29 Data Protection Working Party, Letter to Cherine Chalaby and Goran Marby, 11 December 2017, available here ("At first glance it would seem that since ICANN and the registries jointly determine the purposes and means of processing of personal data for the WHOIS directories, ICANN and the registries are joint controllers. This would mean that both ICANN and the registries must ensure that personal data are processed in accordance with the obligations of the European data protection laws.")

[4] Data Protection Authority (Belgium), Letter to Goran Marby, 4 December 2019, pg. 3, available here.

(joint) controller shall remain accountable for ensuring compliance with data processing operations under its control and cannot abdicate its responsibilities by virtue of a joint agreement."[5]

The guidance and legal advice we have received confirms that a fully centralized model does not shift liability away from contracted parties; rather it expands liability to include the SSAD operator. We must not continue to pursue a system that does not meet the agreed-upon prerequisites for its use.[6] It is time for us as a group to accept the realistic parameters of the system under which the SSAD must operate. Further deliberations on a fully centralized model only distract and delay us from delivering on our work remit in a timely and cost effective manner.

The good news is that we already have all of the legal and practical guidance necessary to immediately develop a hybrid SSAD model that ensures appropriate protection for data subjects, centralizes intake of requests, automates to the greatest extent possible, delegates decision-making to registries and registrars as controllers of personal data, and apportions liability consistent with responsibility for processing.

With the goal of swift progress in mind, the CPH has drafted the attached framework for discussion (*see Attachment 1 - Proposed Hybrid SSAD Model*), which builds on many of the decisions and building blocks already developed by the EPDP team. We stand ready and eager to work with our EPDP colleagues on this proposed path forward and are optimistic that our collective output would be the best possible outcome for the entire community.

This group is at a pivotal moment. Either we accept the advice we have received and start working on a system that is both compliant and implementable, or we continue to avoid and defer the decisions necessary to advance this group's work. The CPH is fully committed to seeing this policy development process through to conclusion and urges other stakeholder groups to join us in agreeing to move forward with a hybrid SSAD model.

Sincerely,

The Contracted Parties House

[5] Data Protection Authority (Belgium), Letter to Goran Marby, 4 December 2019, pg. 3, available here.

[6] Email from Eleeza Agopian on behalf of Goran Marby, 20 February 2019 ("the idea behind this group is to come up with a technical solution that diminishes the contracted parties legal responsibilities . . .")

Attachment 1 - Proposed Hybrid SSAD Model

The proposed hybrid SSAD balances the need for efficiency while still providing for meaningful human review by contracted parties. We recognize that post-GDPR, requestors cite significant challenges in the fragmented approach to requesting non-public registration data from numerous parties. Focusing on centralization, standardization, and automation of the inputs to the system should improve third-parties' ability to access non-public registration data while maintaining contracted parties' oversight and meaningful review of requests (including the flexibility for each contracted party to implement additional automation and standardization based on individual assessments of risk).

The advantages of this approach include:

- **Leveraging existing ICANN systems**: ICANN already operates systems with centralized intake of requests and subsequent routing to registrars and registries. The CZDS system, Naming Services Portal, and Compliance complaint intake process are examples of existing systems built and run by ICANN that already perform the types of functions envisioned for the hybrid model. Using existing systems to the greatest extent possible not only cuts development costs, but should also limit the time necessary to build and launch the system.
- **Standardized inputs:** Standardizing the fields provided with each request should eliminate or significantly decrease the volume of incomplete requests requiring additional communication between the requestor and the contracted party. Standardization also provides predictability for requestors in what is necessary in order to submit a request.
- **Increased transparency and accountability**: Parties submitting requests receive automated confirmation of receipt of the request. Compliance can track the status of requests and take action against parties that do not respond within specified timelines. Third parties making requests are also monitored to ensure that they abide by the terms of service and other safeguards.
- **One-stop shop for all requests:** Request process is less fragmented as requestors can visit one place to make requests.
- **Efficiencies in reviewing and responding:** Responding to requests is more efficient for contracted parties by providing standardized and predictable information needed to make disclosure decisions.
- **Logging & Auditing:** System allows for data collection required for auditing the performance of the system, reporting functions, and compliance of requestors and contracted parties (*see Building Blocks – Logging / Auditing*).
- **Clearly defined roles and responsibilities:** The EPDP can finally answer many of the big conceptual data protection questions about the SSAD, e.g. who are the controllers,

who is responsible for disclosure decisions, and how responsibilities are allocated among the parties.

Disclosure Request Process

The following is a basic framework to begin a functional policy discussion about how requests could be handled as part of a hybrid SSAD model:

1. Requestor visits SSAD.
2. SSAD requires requestor to enter login credentials before gaining access.
    a. Users of the SSAD must be accredited in order to submit a request for disclosure (*see Building Block – Accreditation*).

    b. Credentials for accredited users contain a set of assertions about the user that assist with the verification and authorization of the user (*see Building Block – Accreditation*).

    c. Potential features in the SSAD for accredited users include: (i) retention of required documentation; (ii) pre-populated fields for requests where possible, (iii) acknowledgement of the acceptable use policy (*see Building Block D*), (iv) monitoring/logging of activity; and (v) revocation of access in cases of abuse.

    d. The SSAD may require the functionality to charge a fee for requests based on the decisions made regarding financial sustainability (*see Building Block N*).
3. After credentials are validated, the requestor uses a standardized request process to submit a request for disclosure.
    a. The request process includes a set of standard elements that must be included with each request (*see Building Block A*). Where possible, some of these fields may be pre-populated based on the accreditation/validation of the requestor.

    b. The process may include the ability to indicate an urgent request where necessary or instructions for routing urgent requests outside of the SSAD (*see Building Block G*).

    c. The process includes the ability to upload and attach required documents to the request.

    d. The process should be capable of automated evaluation and confirmation that the request is syntactically correct (*see Building Block G*).
4. The request is routed to the applicable contracted party (consider using the existing Naming Services Portal or building similar functionality) as an open ticket.

5. Contracted party confirms receipt of the request which triggers an automated confirmation notice to the requestor (*see Building Block G*).

    a. No confirmation of receipt after two (2) business days would trigger an automated notification to ICANN for compliance review.

6. Contracted party evaluates and responds to the request in accordance with Building Block G:[7]

    a. Accept the request and provide the data to the requestor (most likely directly in order to avoid ICANN unnecessarily processing personal data).

    b. Deny the request by responding to requestor regarding the rationale for denial.

    c. Deny the request based on insufficient information and send a response back to the requestor requesting specific additional information.

    d. Failure to respond after thirty (30) days triggers an automated notification to ICANN for compliance review.

[7] Note that specific changes are required to the Authorization Provider Building Block based on moving forward with a hybrid model where not all parts of the process (validation of request vs. response to request) are the responsibility of one party.