Registries Stakeholder Group Statement on EPDP Phase II Final Report

The Registries Stakeholder Group ("RySG") appreciates the work done in Phase II, recognizes the utility of an SSAD to third parties, and supports the recommendations contained in the Final Report. The recommendations reflect the EPDP Team's best effort to develop a solution for access to personal data that balances the privacy rights of data subjects with the legitimate interests of third parties. Although this statement addresses concerns about certain aspects of the Final Report, we nonetheless accept the compromises that form the basis of the SSAD recommendations. We remain optimistic about the future development of the SSAD.

During over a year of diligence, Registries have stood firm on the principles that this system must (i) reflect the reality of data protection law as it is today, (ii) prioritize and appropriately protect a registrant's personal data ahead of third party interests, and (iii) retain our ability as controllers to fulfill our legal obligations to protect personal data. Some have noted dissatisfaction with a system based upon these principles. We are nonetheless comfortable standing for these principles as the best way to protect registrants' personal data and fulfill our obligations under law.

RySG Participated in Good Faith

The EPDP was chartered to "determine if the Temporary Specification for gTLD Registration Data should become an ICANN Consensus Policy, as is or with modifications, while complying with the GDPR and other relevant privacy and data protection law."[1] The charter recognizes that the secondary work of evaluating a system for the benefit of third parties to access a registrant's personal data would only begin once the primary issues "were answered and finalized in preparation for the Temporary Specification initial report."[2] A Final Report for Phase I was issued on 19 February 2019, including a detailed and enforceable recommendation for standardizing the process for third parties to obtain a registrant's personal data.[3]

The RySG engaged in Phase II in good faith to develop a system for the benefit of third parties who have a legitimate interest to access a registrant's personal data. Registries do not need such a system in order to fulfill our obligations to protect a registrant's personal data and respond to third party requests to obtain that personal data. Our members are regularly and responsibly responding to data requests today without an SSAD system, in line with the requirements of the Phase I report and our obligations under law. We will continue to do so even once the SSAD is operational. Unfortunately, in many ways the SSAD will make our task more difficult by introducing additional processing and risks to a registrant's personal data.

We listened with an open mind to those communities who insist on more access to personal data and participated in this process in order to find solutions. While we support the Final Report and the many compromises the group has made, for the reasons listed below, we have significant

[1] EPDP Final Adopted Charter – 19 July 2018, available here.
[2] EPDP Final Adopted Charter – 19 July 2018, available here.
[3] *See* EPDP Phase I Final Report, Recommendation 18, available here.

concerns that will require continued diligence moving forward as the community addresses implementation.

RySG Prioritized Data Protection

Our starting point in these discussions has always been data protection principles. Data protection in general, and GDPR specifically, "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."[4] As the EU Commission recently reiterated, "[t]he ultimate objective of the GDPR is to change the culture and behaviour of all actors involved *for the benefit of the individuals*."[5] Simply put, the point of data protection is to protect the personal data of individuals. Although this should be uncontroversial, our experience over the last two years suggests otherwise.[6]

In practice, prioritizing data protection means putting the data subject first when considering the impact of how and by whom their data is processed. It means embracing data minimization and privacy by default as a baseline in order to avoid unnecessary processing of an individual's personal data. It means ensuring that we don't implement policy requirements that restrict our ability as controllers to fulfil our legal obligation to adequately care for personal data that individuals entrust to us.

With these principles in mind, we have still repeatedly shown flexibility and worked to accommodate the interests of third parties, even when doing so required us to make concessions that could increase risk for contracted parties. While some parties would like to have gone further, we must draw the line when we are asked to concede in areas where we have been told repeatedly – by the Phase II independent legal counsel, by data protection authorities, and by our own CPH members with EU data protection expertise – that something is not legally permissible or presents significant risks to the data subject.

The goal of Phase II was to standardize the process for third parties to request a registrant's personal data. However, continued insistence on finding a path to enable virtually automatic access to personal data is not, after many months of analysis, beneficial for data subjects. We are concerned that attempts to pursue automatic access at any cost will ultimately undermine the legality and future viability of the SSAD.

Hybrid Model Reflects Legal and Practical Reality

The hybrid model (i.e., centralized intake with decentralized decision-making) is a practical solution that we believe will solve many of the issues requestors cite with the status quo method

---

[4] GDPR Article 1 (2).

[5] Communication from the Commission to the European Parliament and the Council, European Commission, dated June 24, 2020, p. 5 (emphasis added), available here.

[6] While Article 17 of Charter of Fundamental Rights acknowledges that "[i]ntellectual property shall be protected," European Parliament has clarified that exercise of that right "should not hamper . . . the protection of personal data, including on the Internet." See Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, available here.

of requesting access to registrants' personal data. Most importantly, the hybrid model reflects the reality of what is possible under law today.

Bird & Bird confirmed that liability attaches to controllers of data, and even assuming a fully centralized and automated system that removed discretion from contracted parties, "the most likely outcome – and certainly most supervisory authorities' starting position – is that CPs are controllers."[7] Moreover, the Belgian Data Protection Authority emphasized that controllership is a factual role which the parties "are not free to simply 'designate'" and likewise "cannot abdicate . . . by virtue of a joint agreement."[8]

We accept Bird & Bird and the DPA's advice on this matter, and as far back as January we cautioned that "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."[9] Unfortunately, even in the late stages of the EPDP, we continue to hear suggestions for how certain decision-making about registrant personal data could be centralized and controllership could be assigned by our policy recommendations.[10]

Nothing has changed since the EPDP agreed to reject centralization as not meeting the prerequisite of diminishing liability for contracted parties.[11] We are concerned that some parties either don't understand or willfully ignore legal advice that does not align with their preferred policy outcomes. Either scenario is not ideal for finding consensus on implementable policy recommendations.

Even the term "centralization" doesn't accurately reflect what has actually been proposed by those advocating such a model. Only decision-making, and not the actual data itself, has ever been part of the discussion of a "centralized" system. Without possessing the underlying data, this is not a "centralized" system that would limit unnecessary processing and enhance security for data subjects. Instead, such a system adds additional unnecessary processing steps, and is inconsistent with basic principles of data minimization and privacy by default.

---

[7] Phil Bradley-Schmieg & Ruth Boardman (Bird & Bird LLP), "Questions 1&2: Liability, Safeguards, Controller & Processor", 9 September 2019, p.6, 2.18.

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

[9] CPH Next Steps Letter, dated January 7, 2020.

[10] See, e.g., July 2020 Category 2 Comments on Recommendation 9, IPC/BC proposing "the concept of non-automated by centralized decision making at the CGM" despite legal advice and agreement on a hybrid model: "Per the legal guidance obtained the EPDP Team recommends that the following types of disclosure requests are legally permissible under GDPR for centralized disclosure evaluation (in-take as well as processing of disclosure decision) at the Centralized Gateway Manager when subject to manual processing and review from the start:
· Automated disclosure decisions for clear-cut "domain matching trademark" requests
· Automated disclosure decisions for clear-cut cases of phishing
ICANN org is the controller when processing this disclosure decision."

[11] "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.

We remain concerned about the continued insistence that "centralization" of personal data disclosure is legally permissible or realistic in the ICANN eco-system despite no change in the facts that led us to reject centralization in the first place. While we supported ICANN's efforts to find answers about the allocation of liability under a centralized system, there is still no guidance that indicates that the prerequisite liability shifting is legally possible.

GNSO Standing Committee

The RySG supports the concept that the SSAD should be flexible and able to recalibrate to changed legal or practical circumstances. We recognize that the SSAD must be nimble and able to adapt to an ever shifting landscape of administrative guidance, court decisions, and new regulations in various jurisdictions. We reject, however, the notion that the work of the GNSO Standing Committee must have a predetermined outcome. Namely, we cannot accept the assumption that the SSAD will inevitably evolve towards more centralization and more automation of personal data disclosures in the future. The SSAD must evolve based on facts and data rather than assumptions and conjecture.

As stated above, the hybrid model reflects what is legally possible today. We did not agree to the hybrid model provided it someday evolves into a centralized model because we have no basis to know where the law will go. We agreed to the hybrid model as a solution to improve on the status quo while still adequately protecting individuals' personal data.

The EPDP working group members should set appropriate expectations within their stakeholder groups about how the SSAD may change over time. While this system may move in the direction that some of the EPDP members desire, it is equally (if not more) likely that the system will need to become more restrictive, less automated, or more decentralized.[12] Pitching evolution as a one-way street rather than as responsive to facts and data sets up this system for failure in the eyes of some members of the community.

Similarly, while we have generally supported the scope of the GNSO Standing Committee's work, we have significant concerns about any effort to structure this mechanism in a manner that would cede control of our legal obligations as controllers. We have resisted efforts to state categorically that certain changes, such as adding new automation use cases, are implementation or policy because we cannot predict the shape that future guidance might take on these issues. Unless the European Commission provides perfect, definitive, and unassailable guidance on a topic, automation proposals based on new guidance are likely to have residual risk, additional obligations, or require contractual revisions for contracted parties or the Central Gateway Manager (CGM).

[12] Many of the most significant recent decisions and guidance in this area seem to suggest further restrictions and enforcement rather than a loosening of requirements. *See, e.g.*, Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ("Schrems II") invalidating the EU-U.S. Privacy Shield system; *see also*, Communication from the Commission to the European Parliament and the Council, European Commission, dated June 24, 2020, which calls for increased enforcement of GDPR rather than any relaxation of restrictions, available here.

We can easily imagine cases where even straightforward permissible guidance on additional automation could require policy changes. For example, if new guidance is released that full automation is always permitted provided any entity that has any role in the processing of the data has a designated Data Protection Officer as defined under GDPR. Currently our recommendations do not require any party (CGM, Accreditation Authority, Registries, Registrars, Requestors) to have a Data Protection Officer. In this scenario, if further automation use cases were forced on contracted parties through implementation this could significantly increase contracted parties' legal risks if any of the parties involved in the processing did not appoint a Data Protection Officer.

This example illustrates how important it is that we not pre-determine that changes that are likely to involve legal risk are categorically matters of implementation and not policy. As controllers, we require the ability to be responsive to the obligations that we have to the individuals whose personal data we process.

Full Automation is Only Possible Under Narrow Circumstances

The RySG supports the concept of automation where "technically and commercially feasible and legally permissible."[13] We view those criteria as necessary safeguards to ensure that data subjects are not subject to unreasonable automated processing of their data.

As a starting point, it should be uncontroversial that large scale automation of decisions that impact data subjects - but from which they receive no benefit - is not generally in the best interest of the data subject. As GDPR states, "[t]he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[14] Bird & Bird confirmed for us that, when presented with all possible automation use cases proposed by the team, only four did not produce legal or similarly significant effects for the data subject.[15]

Our take away from that legal advice is that only a very narrowly defined set of decisions do not create a legal or similarly significant effect for data subjects. Similarly, the memo only assesses these use cases under GDPR. As a result, we should be careful about drawing broad conclusions about legal permissibility that will force contracted parties to implement requirements that will increase their legal risk.

[13] EPDP Final Report Phase II, 9.3.

[14] GDPR Article 22.

[15] EPDP Final Report Phase II, 9.4: (i) 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, an Article 2 exemption; (ii) The investigation of an infringement of the data protection legislation allegedly committed by ICANN/Contracted Parties affecting a the registrant by a data protection authority; (iii) Request for city field only, to evaluate whether to pursue a claim or for statistical purposes; (iv) No personal data on registration record that has been previously disclosed by the Contracted Party.

We are also concerned that these four use cases are now required for full automation on day one of the SSAD[16] despite the EPDP Team not even beginning to engage in any technical discussion about how an algorithm can reliably (i) identify requests that are appropriate for automation, or (ii) make decisions in a way that is reliable, accurate, and transparent. We agreed as a plenary that automation had to meet three criteria: (i) technically feasible, (ii) commercially feasible, and (iii) legally permissible.[17] By requiring automation of the use cases in 9.4 on the basis of their legal permissibility, we have collapsed these three important safeguards into a singular assessment of the legality of these use cases.

In fact, the closest we have come to any substantive consideration of how an algorithm could evaluate and make these decisions is the suggestion that the CGM may provide recommendations on disclosure to contracted parties, and that the algorithm would learn from feedback on whether a contracted party's decision to disclose matches the automated recommendation.[18] Not only does this represent a misunderstanding of how machine learning generally works, we have serious doubts about the reliability of recommendations made by a system that does not possess the underlying information that is the basis of our own decisions. Even if our decisions "match" with sufficient regularity, that correlation does not mean that the algorithm is in fact making accurate and reliable decisions.

A much more sophisticated approach to machine learning and algorithm training is needed to assess whether these use cases are technically feasible. This is why requiring technical feasibility as an independent factor is an important part of the consideration of automation use cases. If the parties who now must actually engage in the work of determining technical feasibility and building an algorithm cannot do it successfully, we should not already be locked in to mandatory automation because the technical feasibility requirement has not been met.

Financial Sustainability Requires Attention

From early in Phase II, the RySG advocated for a financial assessment of a proposed SSAD in order to provide important data to guide the EPDP Team's decision-making. We appreciate the work that the ICANN team performed providing us with a cost assessment. In light of ICANN's significant estimated costs for developing and maintaining the proposed SSAD, we are concerned that this assessment is relegated to a single footnote in the Final Report, especially as we continue to observe pushback from other constituencies on the premise that users of the SSAD should bear the costs of operating the system.

To reiterate a point we raised repeatedly during deliberations, under no circumstances should a data subject subsidize the ability of a third party to access their personal data**.** The SSAD is

[16] EPDP Final Report, 9.4: "Per the legal guidance obtained . . . the EPDP Team recommends that the following types of disclosure requests, for which legal permissibility has been indicated under GDPR for full automation (in-take as well as processing of disclosure decision) MUST be automated from the time of the launch of the SSAD . . ."
[17] EPDP Final Report Phase II, 9.3.
[18] EPDP Final Report Phase II, 5.1.1, 5.5.

intended to provide predictable and standardized access to data and should be funded by those who directly enjoy the benefits of such a service.

Furthermore, we support ICANN conducting a cost benefit analysis to determine the financial feasibility of such a system. Considering the extensive work in Phase I to establish a standardized process for third parties to request data directly from contracted parties (Recommendation 18), no party (data subject or third-party requestor) is without a predictable process for requesting personal data. Moreover, any user not wishing to pay for the SSAD service still retains the option of pursuing disclosure requests as established by Phase 1, which is at no cost to the requestor.

In our view, the lack of cost benefit analysis also points to a larger problem: the EPDP never established - beyond anecdotes and conjecture – what the actual problem was that this system is intended to solve. We have seen no reliable data that shows that contracted party responses to requests for disclosure are a problem. Data actually suggests that most appropriately formed queries are responded to and that non-response is generally related to (i) inappropriate requests for data protected by privacy/proxy, or (ii) a lack of response from requestors when additional information is required.[19] The SSAD will not fix either of these requestor mistakes.

Priority 2 Issues Were Addressed

While the RySG supports further work on the Priority 2 issues of Accuracy, Legal vs. Natural, and Feasibility of Unique Contacts, we object to the narrative that these issues were not addressed during Phase II. In fact, each of these issues was addressed in depth, including detailed analysis from Bird & Bird that provides support for maintaining the status quo. We recommend that further work on these topics not start from a blank slate but instead onboard the significant work that the EPDP Team conducted on these topics. We believe it is important to ensure we are transparent and accurate about our consideration of these issues to avoid misconceptions in the community. For example:

Accuracy – Bird & Bird confirmed that accuracy under GDPR is a right of the data subject (and not third parties) and an obligation of the controllers of data.[20] Moreover, Bird & Bird confirmed that the existing procedures under the Registrar Accreditation Agreement for confirming registrant data are not insufficient to meet the requirements for accuracy under GDPR.[21]

Legal vs. Natural – We do not dispute that GDPR applies to natural person and not legal person data. We have emphasized that the practical challenge is reliably determining whether data falls into either bucket, and how to handle legal person records that may contain the data of natural persons. While some have suggested relying on consent as a mechanism to reduce risk, Bird &

---

[19] *See* Privacy and Lawful Access Privacy and Lawful Access to Personal Data at Tucows, 13 March 2020, available here.

[20] Ruth Boardman & Katerina Tassi (Bird & Bird LLP), "Advice on Accuracy Principle under the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"): follow up queries on "Legal vs. Natural" and "Accuracy" memos," dated 9 April 2020.

[21] Ruth Boardman & Gabe Maldoff (Bird & Bird LLP), "Advice on the meaning of the accuracy principle pursuant to the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")," dated 8 February 2019.

Bird confirmed that reliance on consent is not an easy solution and still involves significant risk of liability for contracted parties.[22]

Feasibility of Unique Contacts – We received precise legal guidance on this issue recognizing that while pseudonymization and anonymization are useful privacy enhancing measures, the publication of masked emails would not meet those standards because they are specifically intended to ensure contactability of individuals.[23] Further, we note that the proposed recommendation language on this issue was presented at plenary on March 12, 2020 and received no objection, only to be later omitted from the Final Report.[24]

Controllers Need Flexibility to Fulfill Their Obligations

We support the compromises required to reach agreement on Recommendation 8 (Contracted Party Authorization) but we are concerned that the framework has become too prescriptive. What started off as guidelines for how the disclosing entity MAY make a determination has become rigid in how the disclosing entity MUST make a determination. While Registries support the principle of standardization established by the working group, there is no way for this policy to account for all variations in local jurisdictions with different privacy laws and regulations, particularly when requests are made across borders. Care must be given in implementing and enforcing this recommendation to ensure that the disclosing entity has enough flexibility to account for their specific legal and jurisdictional obligations in order to avoid obviating this recommendation as unenforceable.

Purpose 2

The new Purpose 2 language in Recommendation 22 replaces the original Purpose 2 from EPDP Phase 1 Recommendation 1 which was not agreed to or adopted by the ICANN Board. We reiterate our concern from Phase 1[25] that this purpose does not qualify as a legal "Purpose" as defined in the GDPR.[26] It is not clear that by saying "contribute to the maintenance of the security, stability and resiliency of the Domain Name System in accordance with ICANN's mission" that a

---

[22] Ruth Boardman (Bird & Bird LLP), "Advice on consent options for the purpose of making personal data public in RDS and requirements under the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"),," dated March 2020.

[23] Ruth Boardman (Bird & Bird LLP), ""Batch 2" of GDPR questions regarding a System for Standardized Access/Disclosure ("SSAD"), Privacy/Proxy and Pseudonymized Emails," dated 4 February 2020.

[24] "The EPDP Team agreed to the draft recommendation text for both the feasibility of unique contacts to have a uniform anonymized email address and city field redaction. Staff Support to include these draft recommendations in the addendum on Priority 2 items, which will be published for public comment." Email from Caitlin Tubergen to gnso-epdp-team dated March 12, 2020.

[25] EPDP Phase I Final Report, RySG Phase I Minority Statement, pg. 166, available here.

[26] ICO Guidance on Purpose Limitation: "This requirement aims to ensure that you are clear and open about your reasons for obtaining personal data, and that what you do with the data is in line with the reasonable expectations of the individuals concerned. Specifying your purposes from the outset helps you to be accountable for your processing, and helps you avoid 'function creep'. It also helps individuals understand how you use their data, make decisions about whether they are happy to share their details, and assert their rights over data where appropriate. It is fundamental to building public trust in how you use personal data." Available here.

data subject will understand how their data will be processed or why it is necessary. Noting the above and the Board's support for this purpose[27] and the spirit in which we believe it's intended, the RySG has agreed not to object to this purpose.

Conclusion

The RySG committed to participating actively and in good faith to develop appropriate consensus policy recommendations around access to registrant data. We have focused on ensuring such recommendations provide a clear path to compliance with the GDPR, are commercially reasonable and implementable, take into account our differing business models, and do not inhibit innovation. Consistent with these principles, and noting the concerns detailed above, we provide our consensus support for the Final Report recommendations. We look forward to further consideration and approval by the GNSO Council.

[27] Letter from Martin Botterman to Keith Drazek, dated 11 March 2020, available here.