EPDP Phase 2 Legal Committee Meeting #3

Proposed Agenda

Tuesday, 6 August 14:00 UTC

1. Roll Call & SOI Updates

2. Continued Substantive Review of Updated Priority 1 (SSAD) Legal Questions Submitted to Date

    a) Substantive review of updated SSAD questions
    b) Agree on next steps

3. Wrap and confirm next meeting to be scheduled

    a) Confirm action items
    b) The next LC Meeting will take place on Tuesday, 20 August at 14:00 UTC.

LC Updated Questions

Original Question	Updated Question
2. Answer the controllership and legal basis question for a system for Standardized Access to Non-Public Registration Data, assuming a technical framework consistent with the TSG, and in a way that sufficiently addresses issues related to liability and risk mitigation with the goal of decreasing liability risks to Contracted Parties through the adoption of a system for Standardized Access (Suggested by IPC) 5. Can a centralized access/disclosure model (one in which a single entity is responsible for receiving disclosure requests, conducting the balancing test, checking accreditation, responding to requests, etc.) be designed in such a way as to limit the liability for the contracted parties to the greatest extent possible? IE - can it be opined that the centralized entity can be largely (if not entirely) responsible for the liability associated with disclosure (including the accreditation and authorization) and could the contracted parties' liability be limited to activities strictly associated with other processing not related to disclosure, such as the collection and secure transfer of data? If so, what needs to	Consider a System for Standardized Access/Disclosure where contracted parties "CPs" are required to disclose personal data over RDAP to requestors either directly or through an intermediary request accreditation/authorization body. Assuming the following safeguards are in place, what risk, if any, would the CP face for the processing activity of disclosure in this context? If any risk exists, what improved or additional safeguards would eliminate[1] this risk. In this scenario, would the CP be a controller or a processor[2], and to what extent, if at all, is the CP's liability impacted by this controller/processor distinction? 1. Disclosure is required under CP's contract with ICANN (resulting from Phase 2 EPDP policy). 2. CP's contract with ICANN requires CP to notify the data subject of the purposes for which, and types of entities by which, personal data may be processed. CP is required to notify data subject of this with the opportunity to opt out before the data subject enters into the registration agreement with the CP, and again annually via the ICANN-

[1] "Here it is important to highlight the special role that safeguards may play in reducing the undue impact on the data subjects, and thereby changing the balance of rights and interests to the extent that the data controller's legitimate interests will not be overridden." (https://iapp.org/media/pdf/resource_center/wp217_legitimate-interests_04-2014.pdf)

[2] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

be considered/articulated in policy to accommodate this? (Suggested by GAC)	required registration data accuracy reminder. CP has done so. 3. ICANN or its designee has validated the requestor's identity, and required that the requestor: a. represents that it has a lawful basis for requesting and processing the data, b. provides its lawful basis, c. represents that it is requesting only the data necessary for its purpose, d. agrees to process the data in accordance with GDPR, and e. agrees to standard contractual clauses for the data transfer. 4. ICANN or its designee logs requests for non-public registration data, regularly audits these logs, takes compliance action against suspected abuse, and makes these logs available upon request by the data subject.

4. The question of disclosure to non-EU law enforcement based on Art 6 I f GDPR should be presented to legal counsel. (Suggested by ISPCP)	4. Re question 4, the question is this: European LEAs need to have a legal basis for requesting disclosure. Based on that, they approach the contracted party, which can then disclose based on Art. 6 I c GDPR to fulfil a legal obligation. Where no legal basis for requesting data exists, no disclosure can take place. Art. 6 I c GDPR is limited to European laws. As a consequence, non-EU LEA cannot use a European legal basis for requesting data and the contracted party can therefore not disclose based on 6 I c GDPR. That would leave us with disclosure based on 6 I f GDPR and to the potentially problematic situation in which a domestic European LEA must be able to base its request on a national law while non-EU LEA "only" needs to have a legitimate interest. Remember that even public authorities must not base their processing on 6 I f GDPR in performing their core activities. I trust there is common understanding that investigating crime is the core activity of LEAs and thus it might be a contradiction to have domestic European LEAs blocked from basing their requests on 6 I f GDPR, while non-EU LEA can use that para as a legal basis and also to have the contracted party disclose based on 6 I f GDPR, while in domestic EU cases, only 6 I c GDPR would be applicable. Remember that disclosing data to LEA is much more impactful for the data subject than in civil cases and that therefore, the law makers have included the aforementioned safeguards into the GDPR, which we might be bypassing by using 6 I f GDPR.

	I am not saying this cannot be made work, but we should get confirmation that such disclosure is lawful.
7. To what extent, if any, are contracted parties accountable when a third party misrepresents their intended processing, and how can this accountability be reduced? (BC)	7. To what extent, if any, are contracted parties liable when a third party that accesses non-public WHOIS data under an accreditation scheme where by the accessor is accredited for the stated purpose, commits to certain reasonable safeguards similar to a code of conduct regarding use of the data, but misrepresents their intended purposes for processing such data, and subsequently processes it in a manner inconsistent with the stated purpose. Under such circumstances, if there is possibility of liability to contracted parties, are there steps that can be taken to mitigate or reduce the risk of liability to the contracted parties? (BC)
9. Can legal analysis be provided on how the balancing test under 6(1)(f) is to be conducted, and under which circumstances 6(1)(f) might require a manual review of a request? (BC)	9. Assuming that there is a policy that allows accredited parties to access non-public WHOIS data through an SSAD (and requires the accredited party to commit to certain reasonable safeguards similar to a code of conduct), is it legally possible to have automated disclosures to third parties that have requested access under 6(1)(f)? If it is possible, please provide any guidance for how this can be accomplished. For example, is it legally permissible to define specific categories of requests (e.g. rapid response to a malware attack or contacting a non-responsive IP infringer) to identify types of user groups or processing activities that reduce the need for manual review? In addition, please describe the circumstances (if any) where a manual review is required under 6(1)(f), and any guidance for how to perform this balancing test.

11. Can legal counsel be consulted to determine whether GDPR prevents higher volume access for properly credentialed cybersecurity professionals, who have agreed on appropriate safeguards? If such access is not prohibited, can counsel provide examples of safeguards (such as pseudonymization) that should be considered? (BC)	11. Can legal counsel be consulted to determine whether GDPR prevents fast automated, and non-rate limited responses (as described in SSAC 101) to nonpublic WHOIS data for properly credentialed security practitioners (as defined in SSAC 101), who have agreed on appropriate safeguards? If such access is not prohibited, can counsel provide examples of safeguards (such as pseudonymization) that should be considered? (BC)

12. To identify 6(1)(b) as purpose for processing registration data, we should follow up on the B & B advice that- "it will be necessary to require that the specific third party or at least the processing by the third party is, at least abstractly, already known to the data subject at the time the contract is concluded and that the controller, as the contractual partner, informs the data subject of this prior to the transfer to the third party" B&B should clarify why it believes that the only basis for providing WHOIS is for the prevention of DNS abuse. Its conclusion in Paragraph 10 does not consider the other purposes identified by the EPDP in Rec 1, and, in any event should consider the recent EC recognition that ICANN has a broad purpose to: 'contribute to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission', which is at the core of the role of ICANN as the "guardian" of the Domain Name System." 13. B&B should advise on the extent to which GDPR's public interest basis 6(1)e is applicable, in light of the EC's recognition that: "With regard to the formulation of purpose two, the European Commission acknowledges ICANN's central role and responsibility for ensuring the security, stability and resilience of the Internet Domain Name System and that in doing so it acts in the public interest."	12. Under B&B's memo regarding the applicability of 6(1)(b) as purpose for processing registration data, B & B cites from German commentators that state that it is possible to rely on a contract with the data subject even if controller is not a party to the contract. In that situation, the memo notes that- "it will be necessary to require that the specific third party or at least the processing by the third party is, at least abstractly, already known to the data subject at the time the contract is concluded and that the controller, as the contractual partner, informs the data subject of this prior to the transfer to the third party." Could legal advice be sought on whether an appropriate notice could be drafted to notify the registrant that its non-public WHOIS data will be disclosed to third parties for the purposes identified in ICANN's policy. Under the same memo, B&B's analysis in Section b focuses on only 1 purpose for processing data (DNS abuse), instead of examining all of the purposes identified in the Phase 1 Final Report. In light of the recent EC letters and input to ICANN that clarified how GDPR could be applied to the new WHOIS policy, B&B's prior legal advice should be reexamined and updated. For example, in light of the EC's recognition that ICANN has a broad purpose to: 'contribute to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission', which is at the core of the role of ICANN as the "guardian" of the Domain Name System." and that: "With regard to the formulation of purpose two, the European Commission acknowledges ICANN's central role and responsibility

	for ensuring the security, stability and resilience of the Internet Domain Name System and that in doing so it acts in the public interest." legal advice should be obtained on the applicability of each of the possible legal bases under 6(1) (a-f)) to support the disclosure to third parties under an SSAD of nonpublic WHOIS data.