EPDP Phase 2 Legal Committee Meeting #5

Tuesday, 27 August 14:00 UTC

1. **Roll Call & SOI Updates**
2. **Continued Substantive Review of Priority 1 (SSAD) Legal Questions Submitted to Date**

    a) Substantive review of SSAD questions (beginning where LC left off last week)

- ***Updated Merged Questions 2 and 5*** (proposed by Brian and Thomas):

  Consider a System for Standardized Access/Disclosure where:

  - contracted parties "CPs" are contractually required by ICANN to disclose registration data including personal data,
  - data must be disclosed over RDAP to requestors either directly or through an intermediary request accreditation/authorization body,
  - the accreditation is carried out by third party commissioned by ICANN without CP involvement,
  - disclosure takes place in an automated fashion without any manual intervention,
  - data subjects are being duly informed according to ICANN's contractual requirements of the purposes for which, and types of entities by which, personal data may be processed. CP's contract with ICANN also requires CP to notify data subject about this potential disclosure and third-party processing before the data subject enters into the registration agreement with the CP, and again annually via the ICANN-required registration data accuracy reminder. CP has done so.

  Further, assume the following safeguards are in place

  - ICANN or its designee has validated/verified the requestor's identity, and required in each instance that the requestor:
    - represents that it has a lawful basis for requesting and processing the data,
    - provides its lawful basis,
    - represents that it is requesting only the data necessary for its purpose,
    - agrees to process the data in accordance with GDPR, and
    - agrees to EU standard contractual clauses for the data transfer.

- 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.

1. What risk, if any, would the CP face for the processing activity of disclosure in this context?

2. Would you deem the criteria and safeguards outlined above sufficient to make disclosure of registration data compliant? If any risk exists, what improved or additional safeguards would eliminate[1] this risk?

3. 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?

4. Only answer if a risk still exists for the CP: If a risk still exists for the CP, what additional safeguards might be required to eliminate CP liability depending on the nature of the disclosure request, i.e. depending on whether data is requested e.g. by private actors pursuing civil claims or law enforcement authorities depending on their jurisdiction or the nature of the crime (misdemeanor or felony) or the associated sanctions (fine, imprisonment or capital punishment)?

Footnote 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 [iapp.org])

Footnote 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 [ec.europa.eu]

- ***Updated Question 4*** (proposed by Brian and Volker)*:* Under the GDPR, a data controller can disclose personal data to law enforcement of competent authority under Art 6 1 c GDPR provided the law enforcement authority has the legal authority to create a legal obligation under applicable law.

    a. Can law enforcement agencies of other jurisdictions than the data controller/processor therefore not rely on Art 6 1 c GDPR as a legal basis for the data controller to disclose protected data? Under what circumstances could Art 6 1 c GDPR apply to the disclosure of data in such a context?
    b. Do other legal bases for disclosure exist, besides Art 6I f), that the data controller/processor can rely on for such "foreign" LEAs that lack power to legally compel the data controller/processor?

    Note: awaiting Thomas's addition

- ***Updated Question 11*** (proposed by Margie)*:* Is it permissible under GDPR to provide fast, automated, and non-rate limited responses (as described in SSAC 101) to nonpublic WHOIS data for properly credentialed security practitioners[1] (as defined in SSAC 101) who are responsible for defense against e-crimes (including network operators, providers of online services, commercial security services, cyber-crime investigators) for use in investigations and mitigation activities to protect their network, information systems or services (as referenced in GDPR Recital 49) and have agreed on appropriate safeguards? Or would any automated disclosure carry a potential for liability of the disclosing party, or the controllers or processors of such data? Can counsel provide examples of safeguards (such as pseudonymization/anonymization) that should be considered?

  Footnote 1: SSAC defines "security practitioners" in SSAC 101 as those who have a responsibility to perform specific types of functions (as specified in Section 3) related to the identification and mitigation of malicious activity, and the correction of problems that negatively affect services and users online.

- **Updated Question 12 and 13**: LC to review simplified question before sending to EPDP Team for sign off: In light of the 3 May 2019 correspondence from the European Commission, are any updates on the previous memo on 6(1)(b) necessary?

  - Based on the feedback during the plenary call (question is too broad), would the LC like to propose updated wording to this question?

- ***Question 6:*** *Within the context of an SSAD, in addition to determining its own lawful basis for disclosing data, does the requestee (entity that houses the requested data) need to assess the lawful basis of the third-party requestor? (Question from ICANN65 from GAC/IPC)*

  Note: awaiting updated text from Brian/Georgios

[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

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, 3 September at 14:00 UTC.

Batch 1

1. (Formerly Q7) 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?

2. (Formerly Q9) 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 permissible under Article 6(1)(f) to:

   - define specific categories of requests from accredited parties (e.g. rapid response to a malware attack or contacting a non-responsive IP infringer), for which there can be automated submissions for non-public WHOIS data, without having to manually verify the qualifications of the accredited parties for each individual disclosure request, and/or
   - enable automated disclosures of such data, without requiring a manual review by the controller or processor of each individual disclosure request.

   In addition, if it is not possible to automate any of these steps, please provide any guidance for how to perform the balancing test under Article 6(1)(f).

   For reference, please refer to the following potential safeguards:

   - Disclosure is required under CP's contract with ICANN (resulting from Phase 2 EPDP policy).
   - 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-required registration data accuracy reminder. CP has done so.
   - ICANN or its designee has validated the requestor's identity, and required that the requestor:
     - represents that it has a lawful basis for requesting and processing the data,
     - provides its lawful basis,
     - represents that it is requesting only the data necessary for its purpose,
     - agrees to process the data in accordance with GDPR, and
     - agrees to standard contractual clauses for the data transfer.
   - 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.

3. (Formerly Q12/13) In light of the 3 May 2019 correspondence from the European Commission, are any updates on the previous memo on 6(1)(b) necessary?