**Updated Question 11**

*Status: Thomas, Volker, Brian and Margie to work together on refining this question in advance of the next LC call on Tuesday, 1 October.*

(Previous text 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 practitioners1 (including network operators, providers of online services, commercial security services, private or corporate cyber-crime investigators without public authority (~~as defined in SSAC 101~~) who have voluntarily or under agreement with third parties taken on the responsibility for defense against e-crimes 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 without conducting a balancing test for each individual set of requested data? 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?

In addition, does GDPR prohibit the SSAD to be designed to enable reverse lookups based on contact fields associated with domain names that have been identified as being used for DNS abuse, such as phishing, malware and or similar type of attacks? What are the risks associated with reverse lookups, and if it is possible to conduct reverse lookups, are there steps that can be taken to mitigate any perceived risks?

For purposes of this question, please assume the following safeguards are in place:

o 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.

o 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.

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.~~  are entities that have legal responsibility to protect their technology/network/infrastructure, such as national CERTs, and also DSPs. (See the UK ICO ([https://ico.org.uk/for-organisations/the-guide-to-nis/digital-service-providers/](https://urldefense.proofpoint.com/v2/url?u=https-3A__ico.org.uk_for-2Dorganisations_the-2Dguide-2Dto-2Dnis_digital-2Dservice-2Dproviders_&d=DwMGaQ&c=5VD0RTtNlTh3ycd41b3MUw&r=_4XWSt8rUHZPiRG6CoP4Fnk_CCk4p550lffeMi3E1z8&m=xeXHSQy6Jg3NeENvgZ2sqoBiOr3J07ArOU4MUONzwU4&s=avDrp6cxNXTZKuZCGeGUDM-Cgi0HhyR9IzaQzQAiu3Y&e=)) since these types of companies appear to have security obligations ([https://ico.org.uk/for-organisations/the-guide-to-nis/security-requirements/](https://urldefense.proofpoint.com/v2/url?u=https-3A__ico.org.uk_for-2Dorganisations_the-2Dguide-2Dto-2Dnis_security-2Drequirements_&d=DwMGaQ&c=5VD0RTtNlTh3ycd41b3MUw&r=_4XWSt8rUHZPiRG6CoP4Fnk_CCk4p550lffeMi3E1z8&m=xeXHSQy6Jg3NeENvgZ2sqoBiOr3J07ArOU4MUONzwU4&s=5R4dCyK71voQGm83RO7mPQTr5MU4wMXYqIbyvBJCJUE&e=)).