RrSG Feedback

The RrSG is pleased to note commonalities between this use case and several of the others that the EPDP team has reviewed. There are indeed circumstances where non-public registration data should be provided to third-parties working on abuse prevention and Internet security. We look forward to discussing the patterns that the use case review has surfaced at our face-to-face meeting in LA.

BC-3: Overarching Purpose: Investigate, detect, prevent, and bring civil claims for Abusive Domain names	
The RrSG notes that while law enforcement agencies have the appropriate authority to investigate and detect Abuse, this is not the case for other third parties. Abuse prevention is a shaky legal basis for action, as it relies on an act which has not yet occurred. We do support a use case for bringing civil claims related to domains that are used for Abuse.	

Use Case: Identify owner of abusive domains and other related domains involved in civil legal claims related to phishing, malware, botnets, and other fraudulent activities	
a) User Groups (Requestors) / User characteristics	Law enforcement, operational security practitioners, anti-abuse authorities These groups of people could have very different legal bases to process personal data, and should not be grouped together in this one use case.
b) Why is non-public registration data necessary?	The non-public domain registration data fields (even if inaccurate) provide leads to identify the miscreants and other domain names associated with the miscreants or network of operators of abusive domain names
c) Data elements that may typically be disclosed	• Registrant name, e-mail address, phone, postal address • Technical contact name, email address, phone, postal address As per Phase 1, the Tech Contact no longer has a postal address. • Other domain names linked to the registrant's data contact fields This reverse lookup functionality should not be included in the SSAD. Identifying one domain as a concern does not mean that all other domains with a full or partial match to the registrant's data are problematic or infringing on any rights. For example, a single domain could be hacked or spoofed, or a domain could have someone's data listed on it without permission of the data subject. As

	such, contact data should only be disclosed for pre-identified domains. Additionally, related domains may reveal sensitive personal data (e.g. religious or political affiliation) which must be protected and could result in significant fines if this data is processed improperly. Previous Whois Policy and functionality did not include reverse search as an option. Looking at the "searchability" section in the new gTLD registry agreement, which was referenced in the 6-Sept meeting, we note that searchability is optional for the registry (and is not in any way related to the registrar). We further note that searchability must be limited to only authorized users, and provided in compliance with applicable privacy law. Further, we note that this optional searchability functionality is not widely available.
d) Lawful basis of entity disclosing non-public registration data to the requestor	Disclosure of non-public registration data may be justified under Art. 6 (1) (f) (legitimate interest), (c) performance of contract, (e) (task carried out in the public interest, official authority), and (d) protect the vital interests of the data subject or of another natural person. The establishment, exercise or defense of legal claims is recognized under GDPR as an exception to the rules regarding processing of special categories of personal data under Article 9(2)(f), the right to be forgotten (Art.)17, the right to restriction of processing (Art.18(c)), and the right to object (Art. 21). See also GDPR Recital 52.
e) Supporting info to determine lawful basis for the requestor	Requester should be a trusted notifier or has been vetted and verified by an accreditation body for security practitioners
f) Safeguards (requirements) Applicable to the Requestor	Requestor: ● Must process data in compliance with data protection laws such as GDPR, including secure transmission; ● Must only request current data (no data about the domain name registration's history); ● Must direct requests at the entity that is determined through this policy process to be responsible for the disclosure of the requested data; ● Must provide representations about use of requested data which will be subject to auditing.
g) Safeguards (requirements) applicable to the Entity Disclosing the Nonpublic Registration Data	The entity disclosing the data: ● Must supply only the data requested by the requestor; ● Must return current data in response to a request; ● Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system

	• Must provide data for multiple domain names responsive to the request This should be clarified, as we are not certain if it means that ore than one specific domain can be included in a request, or if it refers to reverse search (on which topic please see our previous comment)
h) Safeguards (requirements) applicable to the data subject This system must be jurisdiction-agnostic, and thus the use case should not refer to one law at the exclusion of others. This section should be revised to be more generally relevant to worldwide data privacy regulations.	The Registered Name Holder (data subject) must have the right: • to obtain, on reasonable request, confirmation of the processing of personal data relating to them and the communication in an intelligible form of the data processed; • to obtain, on reasonable request, rectification or erasure, as the case may be, of inaccurate data This depends on the specific system being created, and must be revisited after that is understood. or data that is being, or has been, processed contrary to the provisions of this Protocol, but in the case of erasure, except where that processing is allowed, necessary, or required under applicable law for: 1. exercising the right of freedom of expression and information; 2. compliance with a legal obligation(s) for the performance of a task carried out in the public interest; 3. the exercise of official authority vested in the controller; 4. reasons of public interest in the area of public health; 5. archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or 6. the establishment, exercise or defence of legal claims. • not to be subject to a decision significantly affecting them based solely on an automated processing of data unless this is: ○ authorized by law providing appropriate safeguards, including at least the right to obtain human intervention; ○ necessary for entering into, or performance of, a contract between the data subject and a data controller; ○ authorized by applicable law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or ○ based on the data subject's explicit consent. Note that whether decisions referred to herein can be made shall always take into account whether applicable law allows for explicit consent or processing necessary for reasons of substantial public interest.

	• to lodge a complaint with the supervisory authority, or authorities, when they consider that their data protection rights have been violated • to an effective remedy before an independent and impartial tribunal when they consider that their data protection rights have been violated. This tribunal concept should be revisited when safeguards are discussed in more detail Note that the right to object will be limited in instances where applicable law allows for (1) the controller to demonstrate compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject or (2) for the establishment, exercise or defence of legal claims or (3) processing where it is necessary for the performance of a task carried out for reasons of public interest.
i) Safeguards (requirements) applicable to the access/disclosure system	• Requests must only refer to current registration data (historical registration data will not be made available via this mechanism). • Contracted parties are only responsible for disclosing nonpublic registration data for the domain names under their management.
j) Accreditation of user group(s) required (Y/N) – if Y, define policy principles	Individuals or entities seeking accreditation as a member of this user group must also: • Agree to only use the data for the legitimate and lawful purpose described above; • Agree to: o the terms of service, in which the lawful use of data described; o prevent abuse of data received; o be subject to de-accreditation if they are found to abuse use of data. • Proof of financial worthiness to justify enhanced access, reverse searching & high volumes (such as bond, letter of credit, insurance, enhanced accreditation fees) Financial status is unrelated to lawful basis for processing data, and should not be a factor.
k) Authentication – policy principles	
l) What information is required to be provided for a request under this lawful basis?	All registration data and domain names requested that are responsive to the request.

m) Expected timing of substantive response	Immediate Data privacy regulations often allow data subjects to opt out of automated processing, and often require that the data subject is informed before their data is processed (e.g. disclosed). This immediate response cannot be required.
n) Is automation of substantive response possible / desirable?	Automation is both possible and desirable.
o) Expected timing of substantive response	Immediate
p) How long can the requestor retain the data disclosed and what are the requirements for destruction following the end of the retention period?	Article 5 (e) of the GDPR states personal data shall be kept for no longer than is necessary for the purposes for which it is being processed.
q) Other?	