|  |
| --- |
| Overarching Purpose: Crime and abuse investigation by non-law enforcement parties.  Recital 49: “The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services.”  Terms:   * Compromise: a domain name, or resources hosted at that domain name, that have been hacked or compromised by a malefactor. * Malicious registration: domain name registered by a malefactor, for the purpose of committing crime or abuse. |
|  |

|  |  |
| --- | --- |
| Use Case: Investigation of criminal activity where domain names are used. Typical specific example: phishing attack. | |
| 1. User Groups (Requestors) / User characteristics | **Parties responsible for defense against e-crime (including network operators, providers of online services, commercial security services, investigators, etc.; may be corporate or academic). Most investigations of this type involve corporate or academic investigators. Law enforcement also rely heavily on these parties.** |
| 1. Why is non-public registration data necessary? | 1. **TASK 1: Determine whether domain is compromised or maliciously registered.** Non-public registration data is needed to determine whether the domain is compromised (registered to a victim registrant, but hacked or hijacked by a malefactor), or if the domain was registered by a malicious party. The difference will determine appropriate mitigation steps.  * For compromised domains: mitigation will involve outreach to registrant and other parties. Domain suspension is to be avoided, to prevent harm to innocent registrant and legitimate services on the domain. * For compromised domains: Reputation providers will not want to blocklist the entire domain. * For maliciously registered domain: domain suspension is a viable mitigation step. * For maliciously registered domain: providers can blocklist the domain.  1. **TASK 2: determine what additional domains may be related**, or involved in the criminal/abusive infrastructure, in order to mitigate and prevent harm.   For example, investigator may determine what IP address the subject domain is on, and find what domains are hosted on that IP. Investigator may then find multiple domains on that IP, and will need to determine which ones are owned by the same registrant.   1. **TASK 3: assemble evidence and rationale for mitigation**. May be for internal use, or to provide rationale to those who can take action. For example, provide evidence so that registrar or registry operator or hosting provider will consider suspending the domain or the abusive activity.   This may involve assessment of the contact data’s accuracy (truthfulness). This process may involve steps such as cross-field validation (does city match postal code, etc.) or comparison to databases of valid physical addresses. Falsified domain registration data is a sign of bad faith.   1. **TASK 4: attribution of crime/abuser to specific actor.** 2. **TASK 5: Report to law enforcement**. (If applicable. See also Recital 50). |
| 1. Data elements that may typically be disclosed[[1]](#footnote-1) | All “public fields” including registrar, Create Data, Nameservers, etc.  The Registrant Contact fields: Name, Organization, Address, Email address, and Phone fields.  For contactability: above fields, plus also, Tech Contact Name, Address, Email address, Phone. |
| 1. Lawful basis of entity disclosing non-public registration data to the requestor | Will include one or more of the following:  6(1)a  6(1)b  6(1)c  6(1)d  6(1)e  6(1)f. See also Recitals 47 and 49. |
| 1. Supporting info to determine lawful basis for the requestor | * 6(1)a and/or 6(1)b and/or 6(1)c, such as in cases where the data subject or a victim are customers or business partners of the investigating entity.   + Examples of this would be customer/victims at an investigating bank, or users of an online service that performs such investigations.   + See also Recital 47 (processing for the purpose of preventing fraud constitutes a legitimate interest)   + Some entities may have legal reporting or regulatory obligations, involving 6(1)c. * 6(1)d. These cases involve child sexual abuse, human trafficking, suicide, missing persons cases, etc. See also Recital 50: “Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller.” * 6(1)e: to be discussed. * 6(1)(f): Third parties can have interests that override the interests of data subjects, as explained in Recital 49. Recital 49 notes network operators have legitimate interests to defend themselves against outside parties, CERTS and providers of security technologies have the legitimate interest to defend parties they serve, etc. |
| 1. Safeguards (requirements) Applicable to the Requestor | The requestor:   1. Must process data in compliance with data protection laws such as GDPR, including secure transmission; 2. Must provide representations about use of requested data which will be subject to auditing. 3. Must log its requests.   Additional items to be considered in the development of a code of conduct[[2]](#footnote-2). Failure to abide by safeguards would affect accreditation, including the possibility of revocation. |
| 1. Safeguards (requirements) applicable to the Entity Disclosing the Nonpublic Registration Data | The entity disclosing the data:   * Must fulfill legitimate requests. * If supplier does not supply the requested data, it must provider a reason why; * A requestor should be able to request and receive both the “public” data fields and the requested non-public fields, rather than just disclosure of the non-public fields. This ensures that any processing is carried out using correct and current information. (And will not require requestors to perform TWO RDS queries about a domain – one of the public fields and one for the private fields.) * Must return current data in response to a request; * Must log requests; * Must respond to legitimate requests and must not rate-limit legitimate requests; * Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system. |
| 1. Safeguards (requirements) applicable to the data subject | 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, per GDPR.   * 1. If the investigator has concluded that the data subject is the perpetrator of a crime, it may not be reasonable to notify (respond to) the data subject. The decision whether to notify the data subject remains with the data controller.   2. Any system designed for disclosing of data under this use case must include a mechanism for communicating the need for confidentiality.   The data controller (registrar) and the Registered Name Holder (data subject) must have the responsibility (under ICANN contract) to respond to notices about inaccurate contact data. |
| 1. Safeguards (requirements) applicable to the access/disclosure system | 1. At this stage of an investigation, bulk access[[3]](#footnote-3), wildcard requests, reverse lookups, and boolean search capabilities are not required. 2. Requests must only refer to current registration data (historical registration data will not be made available via this mechanism). 3. Contracted parties are responsible for disclosing all public and the requested non-public registration data for the domain names under their management. |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles | Some user groups can be accredited.  Qualifications and process to be considered in the development of a code of conduct[[4]](#footnote-4): |
| 1. Authentication – policy principles |  |
| 1. What information is required to be provided for a request under this lawful basis? |  |
| 1. Expected timing of substantive response | These cases are usually related to transient behavior so instant response is critical. Suggest using the RDS SLAs currently contained in ICANN contracts. |
| 1. Is automation of substantive response possible / desirable? | Automation is necessary. |
| 1. Expected timing of substantive response | If party is accredited, then assumption is that data may flow easily. |
| 1. 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 GDPR states that personal data shall be kept for no longer than is necessary for the purposes for which it is being processed.  Deletion following conclusion of investigations should be prompt, although follow-on investigations may occur from time to time. Duration of retention in these cases, and deletion following conclusion of investigations, may be subject to local law related to criminal investigations of this nature. |
| 1. Other? |  |

1. For each request, the requestor will need to confirm which data elements are necessary. [↑](#footnote-ref-1)
2. The code of conduct referenced within this table is distinct from the code of conduct referenced in [Section 3.7.1 of the Registrar Accreditation Agreement](http://www.icann.org/2013raa#3.7.1). [↑](#footnote-ref-2)
3. As defined in section 3.3.6 of the Registrar Accreditation Agreement [↑](#footnote-ref-3)
4. The code of conduct referenced within this table is distinct from the code of conduct referenced in [Section 3.7.1 of the Registrar Accreditation Agreement](http://www.icann.org/2013raa#3.7.1). [↑](#footnote-ref-4)