|  |
| --- |
| Overarching Purpose: Enabling timely resolution of domain-based security events and attacks |

|  |  |
| --- | --- |
| Use Case: When a network is undergoing an attack involving a domain name, and the operator(s) of that network need to contact the domain owner to remediate the security issue (DDOS, Botnet, etc.) | |
| 1. User Groups (Requestors) / User characteristics | **Network Operator(s) and/or their designated network, IT, or operational security teams or providers** |
| 1. Why is non-public registration data necessary? | **Non-Public registration data is required to enable timely contact with those parties responsible for a domain that is being used as an attack vector. Timely communication is essential to reduce downtime and detrimental effects of dependent services.** |
| 1. Data elements that may typically be disclosed[[1]](#footnote-1) | In addition to fields determined to not contain personal data:   * Registrant, Admin and/or Technical contact name * Registrant, Admin and/or Technical contact email * Registrant, Admin and/or Technical contact phone number |
| 1. Lawful basis of entity disclosing non-public registration data to the requestor | Article 6(1)(f) in most cases  Article 6(1)(d) in some cases where critical infrastructure are involved (Example, Mirai Botnet disabled hospitals in UK) <https://healthitsecurity.com/news/icit-finds-healthcare-sector-at-great-risk-for-ddos-attacks> |
| 1. Supporting info to determine lawful basis for the requestor | The need for processing of personal data to the extent necessary is expressly considered in Recital 49.  *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, constitutes a legitimate interest of the data controller concerned.  This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.* |
| 1. Safeguards (requirements) Applicable to the Requestor | The requestor :   * Must process data in compliance with data protection laws such as GDPR, including secure transmission, data subject rights; * Must only request data from the current RDS data set (no data about the domain name registration’s history); * Must provide representations with each unique request for data of its corresponding purpose and legal basis for their processing which will be subject to auditing (no bulk access). |
| 1. Safeguards (requirements) applicable to the Entity Disclosing the Nonpublic Registration Data | The entity disclosing the data:   * Must only supply the data requested by the requestor; * Must return current data in response to a request; * Must process data in compliance with data protection laws such as GDPR, including secure transmission, data subject rights |
| 1. Safeguards (requirements) applicable to the data subject | The Registered Name Holder (data subject):   * Must have their data protected in line with relevant data protection legislation. * May designate a 3rd party (natural or legal persons) to act as their agent to resolve technical issues such as security concerns |
| 1. Safeguards (requirements) applicable to the access/disclosure system | The access/disclosure system:   * Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system, such as unjustified, high-volume automated queries. |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles | With respect to the accreditation of [user groups] seeking accreditation as a member of this user group must provide:  TBD (No current accreditation body exists that adequately includes operational security community)  Additional items to be considered in the development of a code of conduct[[2]](#footnote-2):   * Ability to produce logs / traffic captures that show how the domain was involved in the attack (audit) such that the disclosure was proportional or necessary. |
| 1. Authentication – policy principles |  |
| 1. What information is required to be provided for a request under this lawful basis? | * Domain name * Confirmation of purpose * Acceptance of User Agreement * Accreditation status of requestor (if developed) |
| 1. Expected timing of substantive response | If automated, within seconds. If manual, same day |
| 1. Is automation of substantive response possible / desirable? | Yes |
| 1. Expected timing of substantive response | See above |
| 1. How long can the requestor retain the data disclosed and what are the requirements for destruction following the end of the retention period? | Duration of the attack plus reasonable time to complete AAR. (+30 days?) |
| 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)