|  |
| --- |
| Overarching Purpose:  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. |

|  |  |
| --- | --- |
| Use Case:  Determine “Reputation” of domain name and/or elements associated with domain name registrations.  Operational Description:  Automated reputation system (process) receives domain name or domain name components to evaluate or update. Process accesses the RDS via established access methodology and authentication credentials. Process queries about one or more domain names to retrieve allowed information about the domain name(s) entered. If the starting point is a particular domain attribute like a nameserver or e-mail address, the RDS will create a list of domains with those attributes. Based on the results obtained, the RDS returns a list of domain names and potentially other information the process is entitled to given its credentials. Note that some of the data may be pseudonymized depending upon the request and authorization provided. The process then applies algorithms typically based on stored reputation data to assign reputation values/scores to the domain name(s) or domain name attributes being scrutinized. The process will likely iterate on this case many times based on the information various requests return. | |
| 1. User Groups (Requestors) / User characteristics | Automated process running on system(s) of an authenticated and accredited cybersecurity entity of the RDS system that is obtaining information related to domain name(s) or domain name attributes related to previously identified abusive/criminal activity that impacts the security of networks and confidential information of end users. |
| 1. Why is non-public registration data necessary? | Non-public registration data is requested in order to ascertain domains that are part of criminal infrastructure involved in particular abuse and criminal activities in order to protect networks and end users from criminal and abusive behaviors. |
| 1. Data elements that may typically be disclosed[[1]](#footnote-1) | * Domain Name * Registry Domain ID * Registrar Whois Server * Registrar URL * Updated Date * Creation Date * Registry Expiry Date * Registrar Registration Expiration Date * Registrar * Registrar IANA ID * Registrar Abuse Contact Email * Registrar Abuse Contact Phone * Reseller * Domain Status(es) * Registry Registrant ID * Registrant Fields:   Note: may be pseudonymized   * Name * Organization * Phone * Email * Tech ID * Tech Fields: * Name * Phone * Email * Name Server(s) * DNSSEC * Name Server IP Address(es) * Last Update of Whois Database   A requestor should be able to get both redacted and public information rather than just disclosure of redacted information this ensures that any processing is carried out on correct and current information. |
| 1. Lawful basis of entity disclosing non-public registration data to the requestor | Recital 49  The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security (etc.)  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 provide representations with each unique request for data of its corresponding purpose and legal basis for their processing which will be subject to auditing. These requests may end up producing large data sets, but each must be justified based on actual evidence of abusive/criminal activity. |
| 1. Safeguards (requirements) applicable to the Entity Disclosing the Nonpublic Registration Data | The entity disclosing the data [must] [may]:   * 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] [may]   * Must have their data protected and processed in line with relevant data protection legislation. |
| 1. Safeguards (requirements) applicable to the access/disclosure system | The access/disclosure system [must] [may]   * 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):   * Non-disclosure of audit information to data subject(s) whilst part of an active investigation. |
| 1. Authentication – policy principles |  |
| 1. What information is required to be provided for a request under this lawful basis? | * Domain name(s) * Specific unique data elements for association that may include:   + Registrant e-mail address   + Nameservers   + Registrant ORG   + Tech Contact * Confirmation of purpose * Acceptance of User Agreement * Accreditation status of requestor |
| 1. Expected timing of substantive response | If automated as per SLA if manual 2 business days |
| 1. Is automation of substantive response possible / desirable? | MUST |
| 1. Expected timing of substantive response | If automated as per SLA if manual 2 business days |
| 1. How long can the requestor retain the data disclosed and what are the requirements for destruction following the end of the retention period? | Dependent on processor requirements (e.g. If identified domain names remain active on the Internet, or miscreant continues registering domain name using same data elements identified as unique to that campaign) |
| 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)