|  |
| --- |
| Overarching Purpose:  Criminal Law enforcement/national or public security  A government entity’s authority to investigate, detect, prevent, disrupt, and prosecute criminal activity (including but not limited to terrorism); protect the national security, public safety, public health, or other vital interests of natural persons under a government’s protection; protect against threats to the government, its people, property, or interests; or the exercise of the official or statutory authority vested in a government authority to pursue such activities. |

|  |  |
| --- | --- |
| Use Case:  Investigation of criminal activity against a victim in the jurisdiction of the investigating EU LEA requesting data from a non-local data controller. | |
| 1. User Groups (Requestors) / User characteristics | Criminal Law enforcement/national or public security |
| 1. Why is non-public registration data necessary? | Non-public registration data is requested in order to ascertain if the domain belongs to a secondary victim of a crime or is part of criminal infrastructure involved in the crime and identify further investigatory requirements. |
| 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: * Name * Organization * Street * City * State/province * Postal code * Country * 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 | 6(1)(f) |
| 1. Supporting info to determine lawful basis for the requestor | The GDPR explicitly recognizes the importance of data processing for the “Prevention, investigation, detection or prosecution of criminal offences data processing is also permissible in the event of objection by the data subject. This interest is also explicitly recognized for data transfers to non-EU countries, Art. 49 (1) (e) GDPR. |
| 1. Safeguards (requirements) Applicable to the Requestor (user agreement) | The requestor :   * 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). * Must only use the data for the purpose requested. * Must handle the data subjects personal data in compliance with data protection laws such as GDPR. |
| 1. Safeguards (requirements) applicable to the Entity Disclosing the Nonpublic Registration Data | The entity disclosing the data [must] [may]:   * Must only supply the necessary 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. * Must log requests. * Must define and perform before the processing a balancing test. The data subject should be able to challenge –with proper substantiation- the balancing test with rights to object and to erasure * Must disclose to the Registered Name Holder (data subject), on reasonable request, confirmation of the processing of personal data relating to them, per relevant data protection laws such as GDPR.   + Any system designed for disclosing of data under this use case must include a mechanism for implementing the need for confidentiality for ongoing investigations. |
| 1. Safeguards (requirements) Applicable to the Requestor in an Automatic system(user agreement) | The requestor :   * 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). * Must only use the data for the purpose requested. * Must store, protect and dispose of the data in accordance with any applicable requirements in relevant data protection laws such as GDPR. * May be subject to de-accreditation and/or be reported to an DPA if they are found to abuse the access or use of Data. |
| 1. Safeguards (requirements) applicable to a automatic access/disclosure system | The access/disclosure system [must] [may]   * Must only supply the necessary 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. * Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system. * Must log requests. * Must disclose to the Registered Name Holder (data subject), on reasonable request, confirmation of the processing of personal data relating to them, per relevant data protection laws such as GDPR.   + Any system designed for disclosing of data under this use case must include a mechanism for implementing the need for confidentiality for ongoing investigations. |
| 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:  Dependent on implementation of the standardized system.  Additional items to be considered in the development of a code of conduct[[2]](#footnote-2):   * Non-disclosure of audit information to data subject 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 * Confirmation of purpose * Acceptance of User Agreement * Accreditation status of requestor |
| 1. Expected timing of substantive response | If automated as per SLA (seconds) if manual 2 business days |
| 1. Is automation of substantive response possible / desirable? | Yes |
| 1. Expected timing of substantive response | If automated as per SLA (seconds) 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 (eg. if used as evidence requirement for retention could be twice the length of sentence) |
| 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)