|  |
| --- |
| **Overarching purpose:**  **Criminal Law enforcement**  **A government entity’s authority to investigate, detect, prevent, disrupt, and prosecute criminal activity (including but not limited to terrorism).** |

|  |  |
| --- | --- |
| **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.** | |
| **a)** **User Groups / User characteristics** | **Criminal Law enforcement/national or public security** |
| **b)** **Why is non-public registration data requested?** | **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.** |
| **c) Lawful basis for requesting** | Data processing by competent authorities for the purposes of "prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security" falls outside of the scope of GDPR and is governed by national law setting out the competence of the relevant authorities, including data protection requirements, which for competent authorities from EU Member States are laid down in the national law implementing the data protection directive (2016/680/EU). |
| **d) Lawful basis for disclosing** | Non local data controller: 6(1)(f)  Disclosure of non-public registration data may be justified under Art. 6 (1) (f) GDPR (Legitimate Interest):  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. |
| **e) Lawful basis for processing**  **the disclosed data** | Same a lawful basis for requesting the data |
| **f) Safeguards Applicable to the Entity Disclosing the Nonpublic Registration Data** | * Must only supply 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, such as unjustified, high-volume automated queries. * Must only supply data elements required to suit the purpose |
|  | * Where are safeguards applicable to data subject? |
| **g) Safeguards 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 submit a specific request for every individual domain name (no bulk access); * 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 with requests for data of its corresponding purpose and legal basis for their processing which will be subject to auditing. * Must only request data elements required to fulfill its purpose |
| **h)** **Data elements typically necessary** | Data may have been entered by the criminal actor all fields in RDS are required to aid identification and investigation.  To enable a full assessment of the domain and if belongs to a secondary victim, all fields in RDS are required. |
| **i)** **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; * Only issue disclosure requests with respect to the trademark(s) where ownership is evidenced; * Agree to:   + the terms of service, in which the lawful use of data described;   + prevent abuse of data received;   + be subject to de-accreditation if they are found to abuse use of data or the system to obtain data;   + A register being maintained of all requests with the corresponding purpose and legal basis for their processing (subject to audits).   Failure to abide by safeguards would affect accreditation, including the possibility of revocation. |
| **g)** **Authentication – policy principles** | <need something here> |
| Other? |  |

**Law Enforcement Use Case 2 (EPDP Phase 2 Deliberation)**

|  |  |
| --- | --- |
| **Use Case: Investigation of criminal activity against a victim in the jurisdiction of the investigating EU LEA requesting data from a local data controller.** | |
| **a)** **User Groups / User characteristics** | Criminal Law enforcement/national or public security |
| **b)** **Why is non-public registration data requested?** | Non-public registration data is requested in order to ascertain if the domain belongs to a secondary victim of this crime or is part of the criminal infrastructure and to identify further investigatory requirements. |
| **c) Lawful basis for requesting** | Data processing by competent authorities for the purposes of "prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security" falls outside of the scope of GDPR and is governed by national law setting out the competence of the relevant authorities, including data protection requirements, which for competent authorities from EU Member States are laid down in the national law implementing the data protection directive (2016/680/EU). |
| **d) Lawful basis for disclosing** | For processing falling within the scope of GDPR: 6(1)(c) if request is of mandatory nature; otherwise 6(1)(f)  For processing falling outside the scope of GDPR: national legal basis where required or no legal basis required |
| **e) Lawful basis for processing**  **the disclosed data** | Same basis as for requesting the data |
| **f) Safeguards Applicable to the Entity Disclosing the Nonpublic Registration Data** | * Must only supply 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, such as unjustified, high-volume automated queries. |
| **g) Safeguards 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 submit a specific request for every individual domain name (no bulk access); * 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 with requests for data of its corresponding purpose and legal basis for their processing which will be subject to auditing. |
| **h)** **Data elements typically necessary** | Data may have been entered by the criminal actor all fields in RDS are required to aid identification and investigation.  To enable a full assessment of the domain and if belongs to a secondary victim, all fields in RDS are required. |
| **g)** **Authentication – policy principles** |  |
| Other? |  |