|  |
| --- |
| Overarching Purpose: Criminal Law enforcement/national or public security - Copyright  A government entity’s authority to investigate, detect, prevent, disrupt, and prosecute criminal copyright infringement activity. A single use case is presented with two high level scenarios. The first where the victim is outside of the jurisdiction of the data controller and the second where the victim is in the same jurisdiction of the data controller. |

|  |  |
| --- | --- |
| Use Case: Investigation of criminal activity against a victim in the jurisdiction of the investigating LEA requesting data from either a local 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 criminal copyright infringement.** |
| 1. Data elements that may typically be disclosed[[1]](#footnote-0) | Data may have been entered by the criminal actor thus all fields in RDS are required to aid identification and investigation.   * Registrant Name * Registrant Email Address * Registrant Organization (if available) * Registrant Postal Address * Registrant City * Registrant State/Province * Registrant Postal Code * Registrant Phone Number * Registrant Fax Number * Technical Name * Technical Email Address * Technical Phone Number * <OTHER??>   To enable a full assessment of the domain and an evaluation of whether the parties operating the underlying website should be pursued in a criminal prosecution, all fields in RDS are required. |
| 1. Lawful basis of entity disclosing non-public registration data to the requestor | **Local data controller**  For processing falling within the scope of GDPR: 6(1)(c) if request is of mandatory nature; potentially 6(1)(e)--e.g., EU member state national law requires disclosure of registrant data to LEA as a matter of public interest, or otherwise 6(1)(f)  For processing falling outside the scope of GDPR: national legal basis where required or no legal basis required.  **Non local data controller:**  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. |
| 1. Supporting info to determine lawful basis for the requestor | 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).  According to Article 16 of the Berne Convention, “Infringing copies of a work shall be liable to seizure in any country of the Union [Union here means countries that belong to the Berne Convention, currently 177 countries] where the work enjoys legal protection.” According to Article 14 of the WIPO Copyright Treaty, signatory countries, of which there are currently 95, “shall ensure that enforcement procedures are available under their law so as to permit effective action against any act of infringement of rights covered by this Treaty, including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements.” Furthermore, Article 61 of the Agreement on Trade Related Aspects of Intellectual Property Rights (“TRIPs”) provides “ Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale. Remedies available shall include imprisonment and/or monetary fines sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding gravity. In appropriate cases, remedies available shall also include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale.” Currently, 162 countries are bound by the TRIPS agreement as members of the World Trade Organization. Whether taken individually or together, these international treaties provide a globally recognized basis for criminal enforcement against copyright infringement. As such, these international treaties and agreements that bind the vast majority of the world’s countries clearly provide national law enforcement agencies with globally recognized legitimate authority to criminally enforce copyrights and therefore to request and receive redacted domain name registrant data in cases involving their investigation of potentially criminal copyright infringement of websites operating under the relevant domain name(s) for which the registrant information is requested. |
| 1. Safeguards (requirements) Applicable to the Requestor | The requestor [must] attest that they are a law enforcement or other government agency with responsibility for investigating and/or enforcing criminal copyright infringement |
| 1. Safeguards (requirements) applicable to the Entity Disclosing the Nonpublic Registration Data | The entity disclosing the data [must] [may]: |
| 1. Safeguards (requirements) applicable to the data subject | The Registered Name Holder (data subject) [must] [may] |
| 1. Safeguards (requirements) applicable to the access/disclosure system | The access/disclosure system [must] [may] |
| 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:  [….]  Additional items to be considered in the development of a code of conduct[[2]](#footnote-1):  [….] |
| 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 |  |
| 1. Is automation of substantive response possible / desirable? |  |
| 1. Expected timing of substantive response |  |
| 1. How long can the requestor retain the data disclosed and what are the requirements for destruction following the end of the retention period? |  |
| 1. Other? |  |

1. For each request, the requestor will need to confirm which data elements are necessary. [↑](#footnote-ref-0)
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-1)