|  |
| --- |
| Overarching Purpose: N/A |

|  |
| --- |
| Use Case: Copyright owners requesting data in the establishment, exercise or defense of legal claims for copyright infringement. |
| 1. User Groups (Requestors) / User characteristics
 | Copyright owners, exclusive licensees,their attorneys or agents[[1]](#footnote-0). |
| 1. Why is non-public registration data necessary?
 | Non-public registration data is requested because it is necessary to establish, exercise or defend against legal claims for copyright infringement  |
| 1. Data elements that may typically be disclosed[[2]](#footnote-1)
 | * Registrant Name
* Registrant Email Address
* Registrant Organization (if not published)
* Reginstrant Street
* Registrant City
* Registrant Postal code
* Registrant Phone number
* Registrant Fax number
 |
| 1. Lawful basis of entity disclosing non-public registration data to the requestor
 | Art.6(1)(f) |
| 1. Supporting info to determine lawful basis for the requestor
 | Disclosure of non-public registration data may/ is likely to be justified under Art. 6 (1) (f) GDPR (legitimate interest): The GDPR explicitly recognizes the importance of data processing for the "e*stablishment, exercise or defense of legal claims*". According to Art. 21 (1) GDPR, 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.~~*  Art. 6(1)(f) of the GDPR explicitly applies to the legitimate interests of third parties other than the data controller. Furthermore, it is recognized by the ECJ that the interest to defend individual rights constitutes a legitimate interest for rightsholders to request data (as well as for third parties taking legal action on their behalf).[[3]](#footnote-2) In addition, the UN Declaration of Human Rights expressly recognizes the rights of creators in their works of authorship and explicitly sets forth “the right to protection of the moral and material interests” in such works. (emphasis added).[[4]](#footnote-3) In view of the alleged involvement of the registrant in an infringement and of the recognized interest and right of the author to protect his or her creative works, it cannot be assumed that in these cases that the interests of the registrant in the protection of his data outweigh the interest in the protection of copyrights. Intellectual property is a Fundamental Right under the EU Charter of Fundamental Rights. Copyright law is harmonized globally to a great extent by international agreements (e.g.,Berne Convention, WIPO Copyright Treaty (WCT), WIPO Performances and Phonograms Treaty, Trade Related Aspects of Intellectual Property Rights (TRIPS). Furthermore, in the EU the rights of the data subjects under the GDPR must specifically be balanced against those of the beneficiaries of the exclusive rights under the Copyright Directive (2001) and implementation thereof in national law. Against this background, disclosing redacted registration data to requestors in cases involving the potential infringement of copyrights appears justifiable under Article 6 (1) (f) GDPR.  |
| 1. Safeguards (requirements) Applicable to the Requestor
 | The requestor: 1. Must process data in compliance with data protection laws such as GDPR, including secure transmission;
2. Must provide representations about use of requested data which will be subject to auditing.

Additional items to be considered in the development of a code of conduct[[5]](#footnote-4) (see also section l below):Individuals or entities seeking accreditation as a member of this user group must also:1. Agree to only use the data for the legitimate and lawful purpose described above;
2. Only issue disclosure requests with respect to the copyright(s) they or their principal (if an agent, service provider or trade association) own or control;[[6]](#footnote-5)
3. Agree to:
	* prevent abuse of data received;
	* be subject to de-accreditation if they are found to repeatedly abuse use of data;
	* maintain a register of all requests also including the respective rightsholders name (subject to audits).

Failure to abide by safeguards would affect accreditation, including the possibility of revocation. |
| 1. Safeguards (requirements) applicable to the Entity Disclosing the Nonpublic Registration Data
 | **The entity disclosing the data**:1. Must only supply the data requested by the requestor;
2. May take measures to limit the number of requests that are submitted by the same requestor if it is clear that the requests are not legitimate and of an abusive nature;
3. Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system.
 |
| 1. Safeguards (requirements) applicable to the data subject
 | **The Registered Name Holder** (data subject) must have the right:  1. to obtain, on request, confirmation of the processing of personal data relating to them and the communication in an intelligible form of the data processed;
2. to obtain, on request, rectification or erasure, as the case may be, of inaccurate data or data that is being, or has been, processed contrary to the provisions of this Protocol;

  1. to lodge a complaint with the supervisory authority, or authorities, when they consider that their data protection rights have been violated;
2. to an effective remedy before an independent and impartial tribunal when they consider that their data protection rights have been violated.
 |
| 1. Safeguards (requirements) applicable to the access/disclosure system
 | 1. Unless otherwise required or permitted, the system must not allow bulk access[[7]](#footnote-6), wildcard requests, reverse lookups, nor boolean search capabilities except to the extent reasonably necessary to support the legitimate interests related to this disclosure/use case.
2. Requests must only refer to current registration data (historical registration data will not be made available via this mechanism unless it is within the timeframe for retention of such data as stated in the relevant ICANN contract and compatible with the GDPR data retention requirements).
3. Contracted parties are only responsible for disclosing nonpublic registration data for the domain names under their management;
4. Must receive a specific request for every individual domain name;
5. Must direct requests at the entity that is determined through this policy process to be responsible for the disclosure of the requested data;
 |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles
 | Eligibility criteria for those requesting accreditationWith respect to the accreditation of intellectual property owners, individuals or entities seeking accreditation as a member of this user group must provide:1. An attestation of ownership or grant of exclusive rights in a copyrighted work(s); or
2. Letter of authorization from the rights holders to act on their behalf (in case of attorneys, agents, including trade associations)
 |
| 1. Authentication – policy principles
 |  |
| 1. What information is required to be provided for a request under this lawful basis?
 | 1. Identification of the domain name associated with the website being investigated for copyright infringement.
2. Identification of the copyrighted work claimed to have been infringed, or if multiple copyrighted works at the website are covered by a single request, a representative list of such works relevant to that website.
3. A statement that the requestor has a good faith belief that the website is engaged in infringement of the copyrighted works identified.
4. A statement that the requestor is either the owner or exclusive licensee of rights in the identified copyrighted work(s), or if the requestor is an agent, service provider or trade association, a statement that the requestor is authorized to act on the behalf of the owner or exclusive licensee.
5. Information reasonably sufficient to permit contact with the requestor, such as an email address and telephone number.
6. A statement that the information in the request is accurate.
7. A name and electronic or physical signature of a natural person that is authorized to act on behalf of the requestor
 |
| 1. Expected timing of substantive response
 |  |
| 1. Is automation of substantive response possible / desirable?
 | Automation should be encouraged and implemented wherever technically and commercially feasible |
| 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. Including copyright protection service providers and copyright trade associations that handle copyright matters on behalf of their members. [↑](#footnote-ref-0)
2. For each request, the requestor will need to confirm which data elements are necessary. [↑](#footnote-ref-1)
3. cf. ECJ, case no. C-13/16 (Rigas), rec. 29. [↑](#footnote-ref-2)
4. Art 27(2) of the United Nations Universal Declaration of Human Rights [↑](#footnote-ref-3)
5. 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-4)
6. Unlike trademarks, copyrights exist independent of registration and the leading copyright treaty, the Berne Convention provides in Article 5(2) that “The enjoyment and theexercise of these rights shall not be subject to any formality.” Therefore, unlike in the case of trademarks, evidence of ownership is not an appropriate criteria for copyright. An attestation of the requestor as to ownership of the relevant copyrights by the requestor or by the requestor’s principal would be appropriate; see Section j) below. [↑](#footnote-ref-5)
7. As described in section 3.3.6 of the Registrar Accreditation Agreement [↑](#footnote-ref-6)