|  |
| --- |
| Use Case: Trademark owners processing data in the establishment, exercise or defense of legal claims for trademark infringement |
| 1. User Groups (Requestors) / User characteristics
 | Trademark owners, their attorneys or agents.Other intellectual property rightsholders, such as patent or copyright owners are not considered here. |
| 1. Why is non-public registration data requested?
 | Non-public registration data is requested in order to take legal action against IP law violations through the registration of a domain name |
| c) Data elements typically necessary  |  |
| d) Lawful basis of entity disclosing non-public registration data to the requestor | 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 "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. Although these provisions do not explicitly apply to legal action of parties other than the data controller, 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).[[1]](#footnote-2) In view of the alleged involvement of the registrant in an infringement, it cannot be assumed that in these cases the interests of the registrant in the protection of his data outweigh the interest in the protection of IP rights. IP law is harmonized globally to a great extent by international agreements. Against this background, the possibility of disclosing registration data at a global level appears justifiable under Article 6 (1) (f) GDPR. |

|  |  |
| --- | --- |
| e) Safeguards Applicable to the Requestor | The requestor: 1. Must process data in compliance with data protection laws such as GDPR, including secure transmission;
2. Must only request current data (no data about the domain name registration’s history);
3. Must submit a specific request for every individual domain name (no bulk access);
4. Must direct requests at the entity that is determined through this policy process to be responsible for the disclosure of the requested data;
5. Must provide representations about use of requested data which will be subject to auditing.

 The controller: 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.
 |
| f) Safeguards Applicable to the Entity Disclosing the Nonpublic Registration Data | **The entity disclosing the data**:1. Must only supply the data requested by the requestor;

1. Must return current data in response to a request;

1. 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;
2. 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 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;
3. not to be subject to a decision significantly affecting them based solely on an automated processing of data unless this is authorised by law providing appropriate safeguards, including at least the right to obtain human intervention;
4. to lodge a complaint with the supervisory authority, or authorities, when they consider that their data protection rights have been violated
5. to an effective remedy before an independent and impartial tribunal when they consider that their data protection rights have been violated.
 |
| h) Safeguards applicable to the access/disclosure system | 1. Unless otherwise required or permitted, the system must not allow bulk access[[2]](#footnote-3), wildcard requests, reverse lookups, nor boolean search capabilities.
2. Requests must only refer to current registration data (historical registration data will not be made available via this mechanism).
3. Contracted parties are only responsible for disclosing nonpublic registration data for the domain names under their management.
 |
| i) accreditation of user group(s) required (Y/N) – if Y, define policy principles | With respect to the accreditation of intellectual property owners, individuals or entities seeking accreditation as a member of this user group must provide:1. Evidence of ownership of intellectual property rights (e.g. trademark registration); or
2. Letter of authorization from the rights holders to act on their behalf (in case of attorneys, agents, service providers)

Additional items to be considered in the development of a code of conduct[[3]](#footnote-4): 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 trademark(s) where ownership is evidenced;
3. 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;
	* 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.  |
| j) Authentication – policy principles |  |
| Other? |  |

1. cf. ECJ, case no. C-13/16 (Rigas), rec. 29. [↑](#footnote-ref-2)
2. As described in section 3.3.6 of the Registrar Accreditation Agreement [↑](#footnote-ref-3)
3. 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%22%20%5Cl%20%223.7.1). [↑](#footnote-ref-4)