|  |
| --- |
| Overarching Purpose: Processing personal data to facilitate the UDRP and URS |

|  |  |
| --- | --- |
| Use Case: Processing personal data in the context of UDRP and URS | |
| 1. User Groups (Requestors) / User characteristics | Intellectual property owners, their attorneys or agents[[1]](#footnote-1), and all participants in the UDRP or URS process, including complainants and respondents, panelists, and dispute resolution service providers. |
| 1. Why is non-public registration data necessary? | Non-public registration data is processed to determine (1) against whom, and whether to consolidate, a UDRP or URS complaint; (2) whether an allegedly infringing domain name registrant has acted in bad faith, including, for example, whether the alleged infringer (a) had actual knowledge of the trademark at issue; (b) uses a business name containing the trademark at issue in the WHOIS record; (c) is a competitor of the complainant; (d) is a repeat infringer; (e) maintains other registrations that could form part of a consolidated complaint; (3) whether a potential UDRP or URS dispute may be addressed without the need to file a complaint; and/or (4) whether the registrant might have a legitimate interest in the domain. |
| 1. Data elements that may typically be disclosed[[2]](#footnote-2) | * Registrant   + Name   + Organization (if not published)   + Street   + City   + Postal code   + Phone number   + Fax number   + Email address * Tech   + Name   + Phone   + Email Address |
| 1. Lawful basis of entity disclosing non-public registration data to the requestor | Art. 6(1)(a), Art. 6(1)(b), Art. 6(1)(c), |
| 1. Supporting info to determine lawful basis for the requestor | Art. 6(1)(a): registrant provides informed consent at time of registration and/or renewal. This may need to be more detailed than 2013 RAA requires. Legal advice would be helpful here.  Art. 6(1)(b): contract flows through to registrants in the registration agreement.  Art. 6(1)(c): registries and registrars could be under a legal obligation to disclose personal data to comply with UDRP/URS decisions, and depending on jurisdiction, registries or registrars could be under a legal obligation to disclose personal data to comply with another legal obligation. Such other legal obligation could arise, for example, in a lawsuit appealing the outcome of a UDRP/URS decision. |
| 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. Such representations include agreement to: 3. use the data only for the legitimate and lawful purpose described above; 4. only issue disclosure requests with respect to the trademark(s) where ownership is evidenced and/or with respect to the domain(s) at issue in the dispute; 5. the terms of service, in which the lawful use of data is described; 6. be subject to de-accreditation if they are found to abuse use of data; |
| 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 appropriate action, such as revoking or limiting access to the data if necessary to protect against abuse or misuse of the system, such as unjustified, high-volume automated queries; 3. Must provide, on request from the registrant, confirmation of the processing of personal data relating to them and the communication in an intelligible form of the data processed; 4. Must, on request from the registrant, rectify or erase, as the case may be, inaccurate data or data that is being, or has been, processed contrary to the provisions of this Protocol; 5. Must have a system in place to review and timely act on complaints from registrants that assert their data protection rights have been violated. |
| 1. Safeguards (requirements) applicable to the data subject | **The Registered Name Holder** (data subject):   1. May 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. May 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. May lodge a complaint with the entity disclosing the data, when they consider that their data protection rights have been violated. |
| 1. Safeguards (requirements) applicable to the access/disclosure system | The entity disclosing the data must receive a specific request for every individual domain name (no bulk access**[[3]](#footnote-3)**); |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles | If helpful?  To be productive in this form, proposed criteria follow.  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 demonstrated use); or, 2. A letter of authorization from a trademark rights holder to act on their behalf (in case of attorneys, agents[[4]](#footnote-4)); or, 3. Evidence that a domain dispute complaint has been filed against the individual or entity seeking accreditation; or, 4. Evidence that the individual or entity seeking accreditation is, or is affiliated with, a dispute resolution service provider. |
| 1. Authentication – policy principles | If helpful? |
| 1. What information is required to be provided for a request under this lawful basis? | Required detail in the request, and assent to the data processing agreement as listed above. |
| 1. Exected timing of substantive response | Immediate, or as close to immediate as technically and commercially feasible |
| 1. Is automation of substantive response possible / desirable? | Automation should be encouraged and implemented wherever technically, legally, and commercially feasible |
| 1. How long can the requestor retain the data disclosed and what are the requirements for destruction following the end of the retention period? | The requestor must comply with their obligations under the GDPR and all other relevant privacy regulations. |
| 1. Other? |  |

1. Including brand protection service providers [↑](#footnote-ref-1)
2. For each request, the requestor will need to confirm which data elements are necessary. [↑](#footnote-ref-2)
3. As defined in section 3.3.6 of the Registrar Accreditation Agreement. [↑](#footnote-ref-3)
4. Including brand protection service providers [↑](#footnote-ref-4)