|  |
| --- |
| Overarching Purpose: Preventing Fraud - Consumer Protection.  Terms:   * Primary Actor: Internet users |

|  |  |
| --- | --- |
| Use Case: Online buyers identifying and validating the source of goods or services/ Internet users validating the legitimacy of an email or a website related to a commercial domain name to protect themselves against fraud. | |
| 1. User Groups (Requestors) / User characteristics | **Online buyers, Internet users verifying the legitimacy of an email or a website** |
| 1. Why is non-public registration data necessary? | GDPR expects information on legal persons to be readily available but it is unclear to what extent that will be the case for RDS data. If it is not publically available, Internet users might need the contact information to verify the legitimacy of a commercial domain name |
| 1. Data elements that may typically be disclosed[[1]](#footnote-1) | * Contact information of the commercial domain name: Organization Name, email address, address, and phone number * Contact information of the person selling goods or services: Name, phone number and email address   . |
| 1. Lawful basis of entity disclosing non-public registration data to the requestor | 6(1)(f) |
| 1. Supporting info to determine lawful basis for the requestor | The GDPR specifically mentions fraud prevention as a legitimate interest. Recital 47 says “The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.” We are only talking about commercial domain names and  Recital 14 says “This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person   * People selling goods or services online would typically have their contact information publicly available. However, if this information is not available and is disclosed the registrants' data is used in a way that is reasonably expected and that has minimal privacy impact. * Purpose: Validating the legitimacy of a commercial website or email, fraud prevention Necessity: The user is to mention the reason for which the contact information is required and to prove that it cannot be obtained through other means * Balance: Disclosure of contact information of commercial domain names is reasonably expected by the registrant and has minimal privacy impact |
| 1. Safeguards (requirements) Applicable to the Requestor | The requestor:   1. Is to identify and prove that the requested information belongs to a commercial domain name 2. Is to prove that the contact information is not available through other means 3. Agree to only use the data for the legitimate and lawful purpose described above |
| 1. Safeguards (requirements) applicable to the Entity Disclosing the Nonpublic Registration Data | The entity disclosing the data:   * Must only supply the data requested by the requestor; * Must return current data in response to a request; * Must process data in compliance with data protection laws including but not limited to GDPR |
| 1. Safeguards (requirements) applicable to the data subject | The Registered Name Holder (data subject) must have the right:   1. All rights given under data protection laws including but not limited to GDPR. |
| 1. Safeguards (requirements) applicable to the access/disclosure system | 1. Must receive a specific request for an individual domain name (no bulk access[[2]](#footnote-2)) 2. Boolean search capabilities are not required. 3. Requests must only refer to current registration data (historical registration data will not be made available via this mechanism). 4. Contracted parties are only responsible for disclosing nonpublic registration data for the domain names under their management. 5. Must only return current data related only to the individual requested domain name (no data about the domain name registration’s history);   ; |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles | N |
| 1. Authentication – policy principles |  |
| 1. What information is required to be provided for a request under this lawful basis? | * The requestor contact information * The commercial domain name for which the contact information is required * Proof that the domain name relates to a commercial website or email. * Purpose of request * Who will benefit from the processing * Wider public benefits * Whether the data subject expects the processing of the data in this way or not * Acceptance of the user agreement |
| 1. Expected timing of substantive response | Instant acknowledgement of the request |
| 1. Is automation of substantive response possible / desirable? | Desirable but highly unlikely. |
| 1. Expected timing of substantive response | The requirement to validate request will likely result in relatively poor response timing. |
| 1. Retention period | Until the verification is complete |

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