Following the EPDP Team’s meeting on Thursday 6 June, the staff support team reorganized the user groups overview by focusing on the 3rd party purposes. These 3rd party purposes have been inspired / derived from [the community responses](https://www.icann.org/en/system/files/files/gdpr-dataflow-matrix-responses-redacted-13oct17-en.xlsx) to a request from ICANN org at the end of June 2017 to identify user types and purposes of data elements required by ICANN policies and contracts. It is worth noting that a number of the purposes identified seem to focus on how RDS data was used before the Temporary Specification entered into force and may not necessarily constitute GDPR compliant 3rd party purposes. Also note that the 3rd party purposes identified below do not make a judgement on whether in the case of 6(1)f the balancing test would rule in favor of the user group or the data subject.

As a reminder, per the EPDP Phase 1 recommendation, the Registrar MUST provide an email address or a web form to facilitate email communication with the relevant contact, but MUST NOT identify the contact email address or the contact itself, unless the Registered Name Holder has provided consent for the publication of its email address. However, there is no obligation for the registered name holder to respond and/or to reveal any further information about him/herself or the domain name registration.

This is intended to be a starting point for further EPDP Team deliberations concerning topic c) Define user groups, criteria and purposes / lawful basis per user group. EPDP Team members are requested to review the approach (does this template make logical sense) and 3rd party purposes identified (are these accurate, are there any missing).

Note that the reference in brackets refers to the cell in the community response document. In a number of cases, purposes identified have been defined at a higher level with some examples provided to illustrate specific use cases.

3rd Party Purposes – A user group may have a legitimate interest in requesting the disclosure of registration data to:

* Carry out the obligations and responsibilities of a law enforcement agency;
* Confirm the identity of an entity before completing an online purchase/acquisition;
* Report a technical issue with the domain name;
* Fulfill a licensing or regulatory requirement;
* Carry out academic research, a study and/or statistical analysis;
* Carry out security research;
* Prevent intellectual property infringement;
* Validate domain name ownership for SSL cert requests;
* (for the registrant) Assess what data a controller holds that pertains to their domain name registration.

|  |  |
| --- | --- |
| 3rd Party Purpose: A user group may have a legitimate interest in requesting the disclosure of registration data for the purpose of carrying out the obligations and responsibilities of a law enforcement agency. (Cell *D127, D208, D260, 261, 262*)  Examples:   * To identify contact point for domain name and to gather investigative leads related to the owner/purchaser of the domain; * In order to identify for example, the sources of supply for counterfeit and misbranded medications; individuals engaging in illegal sales of online drugs the individuals responsible for operation of illicit websites associated with counterfeit, misbranded and adulterated Botox. * For the purpose of discovering who operates a given domain and how I can communicate with and/or serve legal process on them in the form of subpoenas and search warrants * In a major fraud investigation, WHOIS lookups were critical to identifying conspirators responsible for registering fraudulent domains. We also have had several groups of individuals using Internet services to lure victims to robberies.  Using a WHOIS lookup is critical to quickly aid us in finding the locations where these defendants are operating from, and have led to subpoenas and eventually to search warrants. | |
| 1. User Groups / User characteristics | Law enforcement and regulatory agencies - a government agency that has investigatory powers and/or is responsible for the enforcement of laws |
| 1. Lawful basis | 6(1)d  6(1)e  6(1)f |
| 1. Data elements typically necessary | Domain Name  IP Address  Name Server  Creation Date  Update Date  Expiry Date  Domain Status  Registrar WHOIS Server  Registrar's URL  Registrar  Registrar Abuse Mail  Registrar Abuse Phone  Reseller  Registrant Name  Registrant Organization  Registrant Street  Registrant City  Registrant State/Province  Registrant Postal Code  Registrant Country  Registrant Phone  Registrant Phone Ext, if available  Registrant Fax, if available  Registrant Fax Ext, if available  Registrant Email  Technical Contact, if available |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles | Yes |
| 1. Authentication – policy principles |  |
| Other? |  |

|  |  |
| --- | --- |
| 3rd Party Purpose: A user group may have a legitimate interest in requesting the disclosure of registration data to confirm the identity of an entity before completing an online purchase/acquisition. *(Cell D2, D122, D257, 258)* | |
| 1. User Groups / User characteristics |  |
| 1. Lawful basis |  |
| 1. Data elements typically necessary |  |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles |  |
| 1. Authentication – policy principles |  |
| Other? |  |

|  |  |
| --- | --- |
| 3rd Party Purpose: A user group may have a legitimate interest in requesting the disclosure of registration data to report a technical issue with the domain name. (*Cell D23, D24, D80, D109*)  Examples:   * Email sending and delivery issues * DNS resolution issues * Web site functional issues | |
| 1. User Groups / User characteristics |  |
| 1. Lawful basis | 6(1)d  6(1)e |
| 1. Data elements typically necessary | Domain Name  IP Address  Name Server  Creation Date  Update Date  Expiry Date  Domain Status  Registrar WHOIS Server  Registrar's URL  Registrar  Registrar Abuse Mail  Registrar Abuse Phone  Reseller  Registrant Name  Registrant Organization  Registrant Street  Registrant City  Registrant State/Province  Registrant Postal Code  Registrant Country  Registrant Phone  Registrant Phone Ext, if available  Registrant Fax, if available  Registrant Fax Ext, if available  Registrant Email  Technical Contact, if available  Account Holder fields |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles |  |
| 1. Authentication – policy principles |  |
| Other? |  |

|  |  |
| --- | --- |
| 3rd Party Purpose: A user group may have a legitimate interest in requesting the disclosure of registration data for the purpose of fulfilling a licensing or regulatory requirement. (Cell *D126*) | |
| 1. User Groups / User characteristics |  |
| 1. Lawful basis |  |
| 1. Data elements typically necessary |  |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles |  |
| 1. Authentication – policy principles |  |
| Other? |  |

|  |  |
| --- | --- |
| 3rd Party Purpose: A user group may have a legitimate interest in requesting the disclosure of registration data for the purpose of academic research, a study and/or statistical analysis. (*Cell D110*)  Includes research on topics such as DNS traffic, data accuracy, botnets, distributed denial of service (DDoS) attacks, and Internet adoption and use. Some are relevant to security and stability purposes. | |
| 1. User Groups / User characteristics | Include: security researchers |
| 1. Lawful basis | 6(1)e  6(1)f |
| 1. Data elements typically necessary | Domain Name  IP Address  Name Server  Creation Date  Update Date  Expiry Date  Domain Status  Registrar WHOIS Server  Registrar's URL  Registrar  Registrar Abuse Mail  Registrar Abuse Phone  Reseller  Registrant Name  Registrant Organization  Registrant Street  Registrant City  Registrant State/Province  Registrant Postal Code  Registrant Country  Registrant Phone  Registrant Phone Ext, if available  Registrant Fax, if available  Registrant Fax Ext, if available  Registrant Email  Technical Contact, if available |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles |  |
| 1. Authentication – policy principles |  |
| Other? |  |

|  |  |
| --- | --- |
| 3rd Party Purpose: A user group may have a legitimate interest in requesting the disclosure of registration data for the purpose of security operations, investigations, and research. (*Cell D550, D555*)  Examples include but are not limited to:   * “ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems….This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems“ (Recital 47) * Use data elements of known malicious sites to find correlations between entities and and domains how they are linked; calculate a score based on an algorithm that identifies sites with a high probability of being malicious ; maintain Reputation Block Lists (RBLs) and domain reputation scoring mechanisms * Maintain protective systems, such as firewalls. * Find, investigate, and mitigate DNS abuse * Determine identity of malicious actor, or determine identity of a victim * Investigate crimes, and report possible criminal acts or threats to public security to authorities. * Detect fraud. Evaluate data accuracy. * Security investigations and operations are often undertaken by or on behalf of data controllers. Others are undertaken by or on behalf of affected parties. | |
| 1. User Groups / User characteristics | those who have a responsibility to perform the above types of functions. These include network operators; those running commercially available products and services; registry operators who run anti-abuse programs in their TLDs; law enforcement personnel and private investigators; etc. |
| 1. Lawful basis | 6(1)c  6(1)d  6(1)e  6(1)f  See also Recitals 47, 49, and 50 |
| 1. Data elements typically necessary | Domain Name  IP Address  Name Server  Creation Date  Update Date  Expiry Date  Domain Status  Registrar WHOIS Server  Registrar's URL  Registrar  Registrar Abuse Mail  Registrar Abuse Phone  Reseller  Registrant Name  Registrant Organization  Registrant Street  Registrant City  Registrant State/Province  Registrant Postal Code  Registrant Country  Registrant Phone  Registrant Phone Ext, if available  Registrant Fax, if available  Registrant Fax Ext, if available  Registrant Email  Technical Contact, if available |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles |  |
| 1. Authentication – policy principles |  |
| Other? |  |

|  |  |
| --- | --- |
| 3rd Party Purpose: A user group may have a legitimate interest in requesting the disclosure of registration data for the purpose of preventing intellectual property infringement. (*Cell D265, D290, D315, D340, D383, D408, D435, D563*)  Examples:   * In order to enable contact with parties using a domain name that is being investigated for trademark/brand infringement or copyright theft; * To Combat Fraudulent Use of Registration Data by facilitating identification of and response to fraudulent use of legitimate data (e.g., address) for domain names belonging to another Registrant by using Reverse Query on identity-verified data * To verify domain name and contact information in order for the UDRP Provider to abide by the rules as delineated in the UDRP. This includes: 1) Complaint verification, 2) Determining the Registrar, 3) Completing the administrative compliance check, 4) determining the jurisdiction to seat the panel, and 5) post panel decision logistics. (informing registrar, registrant and ICANN) * In order to accurately identify and/or confirm other web domains used in connection with defendant(s) alleged IP infringements (including whether previous actions taken against registrant). As well as to facilitate the service of legal process by hand-delivery, mail service or service by email. | |
| 1. User Groups / User characteristics |  |
| 1. Lawful basis |  |
| 1. Data elements typically necessary |  |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles |  |
| 1. Authentication – policy principles |  |
| Other? |  |

|  |  |
| --- | --- |
| 3rd Party Purpose: A user group may have a legitimate interest in requesting the disclosure of registration data for the purpose validating domain name ownership for SSL cert requests. (D125, D608) | |
| 1. User Groups / User characteristics |  |
| 1. Lawful basis |  |
| 1. Data elements typically necessary |  |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles |  |
| 1. Authentication – policy principles |  |
| Other? |  |

|  |  |
| --- | --- |
| 3rd Party Purpose: A user group may have a legitimate interest to request what data a controller holds that pertains to their domain name registration. (D98) | |
| 1. User Groups / User characteristics |  |
| 1. Lawful basis |  |
| 1. Data elements typically necessary |  |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles |  |
| 1. Authentication – policy principles |  |
| Other? |  |