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 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.

The CPH has significant concerns around providing specific examples of circumstances where law enforcement may get access. It is enough to simply state that law enforcement MUST assert a specific legal right for access; providing examples is unnecessary. The sole exception to requiring a 'legal' basis is when there are vital interests, and as per ICO this means threat to life, which has not been referenced here.

a) User Groups / User characteristics	Law Enforcement Agencies - a government agency that is responsible for the enforcement of laws
b) Lawful basis	6(1)e 6(1)f (in very limited cases) The inclusion of 6(1)f as a lawful basis is incorrect and must be removed. The final line of Article 6(1) states "Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks" and this includes law enforcement agencies. Should a member of law enforcement wish to make a request under Article 6(1)f, it would not be under the auspices of the law enforcement agency.
c) 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

	All of the above are not personal data relating to a domain and should not be mentioned here. These data are available publicly. 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
d) Accreditation of user group(s) required (Y/N) – if Y, define policy principles This assumes the context of a centralized system. The question should be 'would accreditation be helpful?' as it is certainly not required. Only authentication/verification, to an extent, would be required.	Yes
e) 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)* The CPH does not support this being listed as a purpose. The issue can be solved through EV or OV SSL certificates, or a TXT record in the DNS. With regards to ownership of a domain name, an online store could for example be owned by someone entirely different & thus disclosure is invalid for this purpose. How would the requestor demonstrate that they are actually purchasing from that website? The legitimate purpose relates to the individual request and not a class of requests.	
a) User Groups / User characteristics	
b) Lawful basis	
c) Data elements typically necessary	
d) Accreditation of user group(s) required (Y/N) – if Y, define policy principles	
e) 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***) The CPH does not support this being listed as a purpose. Unlike in the 80s and 90s, Registrars are obligated to have a contact form or forwarding email in the public RDS response, so there is no need to disclose personal data in order to facilitate reporting of technical issues to the domain owner The inclusion of this as a suggested purpose demonstrates the need to assess necessity as a part of the balancing test. Release of personal data for this purpose, where a path for the forwarding of a communication to that contact already exists, must defeat the disclosure request, unless it can be shown that this path was first followed, but the issue still persists (and even then the issue must be of a quality to necessitate disclosure - a simple and non-important error may still result in a denial of disclosure). Examples: • Email sending and delivery issues • DNS resolution issues • Web site functional issues	
a) User Groups / User characteristics	
b) Lawful basis	
c) Data elements typically necessary	
d) Accreditation of user group(s) required (Y/N) – if Y, define policy principles	
e) 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***) The CPH does not support this being listed as a purpose. A domain owner can publish the data (and registrars are obligated to offer that option) or they can disclose it to the licensing / regulatory board themselves. This is another example of the legal basis is a 6(1)f and does not need to be a user group. The focus when reviewing these third-party purposes should be the rights of the data subject and not the needs of 3rd parties.	
a) User Groups / User characteristics	
b) Lawful basis	
c) Data elements typically necessary	
d) Accreditation of user group(s) required (Y/N) – if Y, define policy principles	

e) 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***)

The CPH does not support this being listed as a purpose. The terms 'academic research, study and/or statistical analysis' are too non-specific, there is no way to authenticate those involved. It may also include commercial data which is not appropriate for publication.

It is up to the requester to establish that they have a legitimate basis (research), with a valid legal basis, and that the disclosure of data is necessary in the context of that particular study. Being a researcher does not give any special pass (even accredited); if the research represents an unnecessary interference with the data subject's rights, the disclosure must be denied

Research done by the data controller itself has a special place in data protection - this is not the research of a 3rd party. Research would therefore just be a 6(1)f request.

This user group does not help make this process any more streamlined; it just creates a false impression of such requests being somewhat more privileged, which they are not.

a) User Groups / User characteristics	
b) Lawful basis	
c) Data elements typically necessary	
d) Accreditation of user group(s) required (Y/N) – if Y, define policy principles	
e) 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 research. (***Cell D550, D555***)

The CPH does not support this being listed as a purpose. There is no standalone legal basis for requesting personal data for the purpose of security research; such a request would still need to pass the 6(1)f balancing test..

Examples:

- A security researcher may use data elements of known malicious sites to build a map of entities and how they are linked, adding additional related public external information, e.g., autonomous system numbers (ASNs), in search of related domains that will have a high probability of being malicious.
- A security researcher may use data elements of an unknown site to calculate a score based on a proprietary algorithm that identifies sites with a high probability of being malicious.

a) User Groups / User characteristics	

b) Lawful basis	
c) Data elements typically necessary	
d) Accreditation of user group(s) required (Y/N) – if Y, define policy principles	
e) 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*)

The CPH believes the language here should be amended as disclosure does not 'prevent' IP infringement - it can help with suing a person, or taking legal action in various ways, but not 'preventing' the infringement. As the purpose should not effectively permit fishing expeditions, it should be reworded as a purpose of 'responding to' IP infringement.

Owning a Trademark does not confer special rights to non-public data. It is not up to Contracted Parties to facilitate investigations against domains that contain a TM. The key here is

necessity. If a company wishes to protect their IP, generally speaking, the identity of the registrant is not necessary to constitute such proceedings. Such proceedings, as a matter of course, may include a simple discovery motion. Contracted parties shall then disclose under 6(1)c (in jurisdiction) or perhaps 6(1)f when outside of jurisdiction.

There are also those fringe cases where actual damage is likely to occur
as a result of the infringement (subjective case review based on individual circumstances e.g. phishing, spear phishing etc.). A 6(1)f may be sufficient in such circumstances.

In truth, the issue here is that the 'legitimate purpose' is based on the individual circumstance of the request; requests are not 'legitimate' because they are TM/IP related, but because the circumstances of that request are supporting disclosure. The CPH cautions against presupposing outcomes in purporting to classify any such niche interest as 'legitimate' in general terms. This goes for all categories identified and not just IP/TM.

Examples:

- In order to enable contact with parties using a domain name that is being investigated for trademark/brand infringement or copyright theft;
  This can be achieved via the public RDS (registrars are obligated to allow contact of RNH)
- 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
  The CPH believes this example should be removed as it is not compliant with data protection law; there should be no reverse search. Researchers can use other means to make useful connections to domain names involved in cyber crime. This use case is very narrow and assumes that cyber criminals re-use the registration data over and over which is often NOT the case. Creating fake data is as easy as clicking a button; https://cyber-hub.net/fake_info.php

- 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)
  The CPH believes this example should be removed as it is no longer needed. The UDRP case can be filed with only public info & the UDRP Provider already confirms domain ownership data with the Registrar
- 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.
  The CPH believes this example should not include 'previous actions taken against a registrant' as there is no reverse search.

a) User Groups / User characteristics	
b) Lawful basis	
c) Data elements typically necessary	
d) Accreditation of user group(s) required (Y/N) – if Y, define policy principles	
e) 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 validating domain name ownership for SSL cert requests. (D125, D608)
The CPH does not support this being listed as a purpose. There are other technical methods to achieve this and Cert Providers have modified their processes already. Domain name ownership could instead be verified by adding info in DNS (like the TXT record)

a) User Groups / User characteristics	
b) Lawful basis	
c) Data elements typically necessary	
d) Accreditation of user group(s) required (Y/N) – if Y, define policy principles	
e) 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)
The CPH does not support this being listed as a purpose. If this is in reference to the data subject, then the Controller already has an access process in place. A data subject does not

need to be a SSAD user to request this data, and in fact we should stop considering them as one of the 'users' and more as the only party who has rights in this situation.

If it's a third party then they would need to fall under one of the relevant purposes listed above.

a) User Groups / User characteristics	
b) Lawful basis	
c) Data elements typically necessary	
d) Accreditation of user group(s) required (Y/N) – if Y, define policy principles	
e) Authentication – policy principles	
Other?	