Third Party Legitimate Interest	Comments received
i. Carry out the obligations and responsibilities of a law enforcement agency 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.	**Contracted Party House**: 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.
ii. Confirm the identity of an entity before completing an online purchase/acquisition	**Contracted Party House**: 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.
iii. Report a technical issue with the domain name	**Contracted Party House**: 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).
iv. Fulfill a licensing or regulatory requirement	**Contracted Party House**: 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.
v. Carry out academic research, a study and/or statistical analysis	**SSAC:** 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. **Contracted Party House**: 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.
vi. Carry out security operations, investigation, and research 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.	**SSAC:** 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. **Contracted Party House**: 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.
vii. Prevent intellectual property infringement 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.	**Contracted Party House:** 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.

	(first bullet) This can be achieved via the public RDS (registrars are obligated to allow contact of RNH) (second bullet) 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 (third bullet) 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 (fourth bullet) The CPH believes this example should not include 'previous actions taken against a registrant' as there is no reverse search.
viii. Validate domain name ownership for SSL cert requests	**Contracted Party House:** 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)
ix. A user group may have a legitimate interest to request what data a controller holds that pertains to their domain name registration.	**Contracted Party House:** 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.