Use Case: Trademark owners requesting data to take legal action against cybersquatters	
a) User Groups / User characteristics	Trademark owners, their attorneys or agents. Other intellectual property rightsholders, such as patent or copyright owners are not considered here.
b) Why is non-public registration data requested?	Non-public registration data is requested in order to take legal action against IP law violations through the registration of a domain name
c) Lawful basis	Disclosure of non-public registration data may be justified under Art. 6 (1) (f) GDPR (legitimate interest): The GDPR explicitly recognizes the importance of data processing for the "e*stablishment, exercise or defense of legal claims*". According to Art. 21 (1) GDPR, data processing is also permissible in the event of objection by the data subject. This interest is also explicitly recognized for data transfers to non-EU countries, Art. 49 (1) (e) GDPR. Although these provisions do not explicitly apply to legal action of parties other than the data controller, it is recognized by the ECJ that the interest to defend individual rights constitutes a legitimate interest for rightsholders to request data (as well as for third parties taking legal action on their behalf).[1] In view of the alleged involvement of the registrant in an infringement, it cannot be assumed that in these cases the interests of the registrant in the protection of his data outweigh the interest in the protection of IP rights. IP law is harmonized globally to a great extent by international agreements. Against this background, the possibility of disclosing registration data at a global level appears justifiable under Article 6 (1) (f) GDPR.
d) General safeguards	In order to comply with the fundamental principles of European data protection law, in particular the principle of data minimization limiting any data processing to the extent necessary for the fulfilment of a specific purpose (Article 5 (1)(c) GDPR), a number of general preconditions must be met: • Accredited users may only request current data (no data about domain history) • Only data of a single domain can be viewed at the same time • Accredited parties are not provided with bulk access • No boolean search functionality is provided to accredited users • No search functions are offered for data elements other than the domain name • No reverse lookups are offered

[1] cf. ECJ, case no. C−13/16 (Rigas), rec. 29.

	• Disclosure requests must be directed at the contracted party that holds the requested data (at least as long as no central system is operational) • Volume limitations / slowed down response times / captchas shall be implemented to avoid mass lookups or automated lookups
e) Data elements typically necessary	As legal action against the registrant is the reason for the request and justification for disclosure, only the registrant data may be disclosed. Registrant name, organization (if not published) and postal address appear to be sufficient for this in order to serve legal writs. Our group should discuss whether phone number, fax number or e-mail address are required to be disclosed.
f) Accreditation of user group(s) required (Y/N) – if Y, define policy principles	In addition to the measures described above and in order to mitigate risks for abusive use of non-public registration data third parties must be able to provide or (should this be implemented technically) provide such information prior to individual lookups - evidence of ownership of intellectual property rights (e.g. trademark registration); or - letter of authorization from the rights holders to act on their behalf (in case of attorneys, agents) Furthermore, this third party group must - agree to use the data for the legitimate and lawful purpose described above - only issue disclosure requests with respect to the trademark(s) where ownership is evidenced - agree to o the terms of service, in which the lawful use of data described; o prevent abuse of data received; o be subject to de-accreditation if they are found to abuse use of data; o maintain a register of all requests also including the respective rightsholders name (subject to audits).
g) Authentication – policy principles	
Other?	