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 to protect themselves	
a) User Groups (Requestors) / User characteristics	**Online buyers, Internet users verifying the legitimacy of an email or a website**
b) Why is non-public registration data necessary?	Typically contact information of legal persons is publically available. However, if it is not publically available, Internet users might need the contact information to verify the legitimacy of a commercial domain name
c) Data elements that may typically be disclosed[1]	• Contact information of the commercial domain name: Company Name, Address, and phone number • Contact information of the person selling goods or services: Name, phone number and email address .
d) Lawful basis of entity disclosing non-public registration data to the requestor	6(1)(f)
e) Supporting info to determine lawful basis for the requestor	The GDPR specifically mentions fraud prevention as a legitimate interest • People selling goods or services online would typically have their contact information publically 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: 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
f) Safeguards (requirements) Applicable to the Requestor	The requestor: **1.** Is to identify 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] For each request, the requestor will need to confirm which data elements are necessary.

g) 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;
h) Safeguards (requirements) applicable to the data subject	The Registered Name Holder (data subject) must have the right: 1. All rights given under the GDPR
i) Safeguards (requirements) applicable to the access/disclosure system	1. Boolean search capabilities are not required. 2. Requests must only refer to current registration data (historical registration data will not be made available via this mechanism). 3. Contracted parties are only responsible for disclosing nonpublic registration data for the domain names under their management. 4. Must only return current data (no data about the domain name registration's history); **5.** Must receive a specific request for every individual domain name (no bulk access[2]);
j) Accreditation of user group(s) required (Y/N) – if Y, define policy principles	N
k) Authentication – policy principles	
l) What information is required to be provided for a request under this lawful basis?	The requestor contact information Why the data is required Who will benefit from the processing Are their wider public benefits Does the registrant expect the processing of the data in this way
m) Expected timing of substantive response	instant acknowledgement of the request
n) Is automation of substantive response possible / desirable?	Automation, if possible, is highly desirable.
o) Expected timing of substantive response	As per (m) above, the decision of the data controller whether to disclose the data should be given the highest priority.
p) Retention period	Until the verification is complete

[2] As defined in section 3.3.6 of the Registrar Accreditation Agreement.

Overarching Purpose: Fraud Prevention – Consumer Protection **Terms:** • Primary Actor: **Consumer Protection Organizations**	
Use Case: Consumer protection organizations	
q) User Groups (Requestors) / User characteristics	**Consumer Protection Organizations**
r) Why is non-public registration data necessary?	To conduct investigations of Internet scams and stop perpetrators of fraud and spam from infecting consumers' computers or harming them.
s) Data elements that may typically be disclosed[3]	• Contact information of the domain name: Company Name, Address, and phone number • Contact information of the person selling goods or services: Name, phone number and email address .
t) Lawful basis of entity disclosing non-public registration data to the requestor	6(1)(c) 6(1)(e) 6(1)(f)
u) Supporting info to determine lawful basis for the requestor	6(1)(c) law enforcement agencies 6(1)(e) can be used by organizations • Carrying out specific tasks in the public interest, which is laid down by law • Exercising official authority which is laid down by law 6(1)(f) • Private sector organizations • Public authorities, if the processing is outside their tasks
v) Safeguards (requirements) Applicable to the Requestor	The requestor: • For public authority organizations: Identify if the processing is necessary for a relevant task that is clearly set out in law • For nonpublic authority organizations or if the processing is not part of the public authority tasks specify the reason for disclosure • Prove that the requested information is not available through other means • Agree to only use the data for the legitimate and lawful purpose described above
w) Safeguards (requirements) applicable to the Entity	The entity disclosing the data: • Must only supply the data requested by the requestor;

[3] For each request, the requestor will need to confirm which data elements are necessary.

Disclosing the Nonpublic Registration Data	• Must return current data in response to a request;
x) Safeguards (requirements) applicable to the data subject	The Registered Name Holder (data subject) must have the right: All rights given under GDPR
y) Safeguards (requirements) applicable to the access/disclosure system	6. Boolean search capabilities are not required. 7. Requests must only refer to current registration data (historical registration data will not be made available via this mechanism). 8. Contracted parties are only responsible for disclosing nonpublic registration data for the domain names under their management. 9. Must only return current data (no data about the domain name registration's history); **10.** Must receive a specific request for every individual domain name (no bulk access[4]);
z) Accreditation of user group(s) required (Y/N) – if Y, define policy principles	Y It is preferable that consumer protection organizations are accredited. Accreditation can be revoked if the disclosed data is misused
aa) Authentication – policy principles	
bb) What information is required to be provided for a request under this lawful basis?	Why the data is required Who will benefit from the processing Are their wider public benefits
cc) Expected timing of substantive response	instant acknowledgement of the request
dd) Is automation of substantive response possible / desirable?	Automation, if possible, is highly desirable.
ee) Expected timing of substantive response	As per (m) above, the decision of the data controller whether to disclose the data should be given the highest priority.
ff) Retention period	Until the verification is complete

[4] As defined in section 3.3.6 of the Registrar Accreditation Agreement.