Domain name data disclosure policy in the .lv top-level domain

Riga, 25. 08.2026

1. Purpose

The purpose of this Domain Name Data Disclosure Policy (hereinafter - the Disclosure Policy) is to establish the principles and general conditions under which the Registry Operator for the .lv top-level domain and .lv Registrars disclose registration data concerning Registrants to third parties, in compliance with applicable laws and regulations.

2. Scope

2.1. The Disclosure Policy applies to registration data concerning .lv domain names that are not publicly available through the NIC Whois service and to all data disclosure requests received from:

2.1.1. law enforcement authorities and other state institutions and public law entities, for the performance of functions assigned to them by laws and regulations, for the purpose of preventing and combating domain name system abuse, as well as preventing and detecting cyber incidents;

2.1.2. institutions responsible for the prevention of cyber incidents, for the performance of functions assigned to them by laws and regulations, for the purpose of preventing and combating domain name system abuse, as well as preventing and detecting cyber incidents

2.1.3. other private law entities, where a legal justification is provided and in cases involving infringements of the domain name system in the field of private law.

2.2. The Disclosure Policy shall be applied by the Registry Operator for the .lv top-level domain and .lv Registrars.

2.3. According to the definition adopted by the Internet Corporation for Assigned Names and Numbers (ICANN), domain name system abuse comprises the following technical infringements associated with a specific domain name:

2.3.1. Botnets[i],

2.3.2. Malware[ii],

2.3.3. Pharming[iii],

2.3.4. Phishing[iv],

2.3.5 Spam[v], where used as a delivery mechanism for the above forms of DNS abuse.

3. General principles of data disclosure

3.1. Data shall be disclosed only where the request for disclosure of domain name data is legally justified and complies with the principles of data minimisation and proportionality.

3.2. Data shall be disclosed only for specific, legitimate purposes consistent with the stated legal basis.

3.3. Data shall not be disclosed where disclosure could pose an unjustified risk to the rights of the Registrant or where the request is insufficiently substantiated.

3.4. All instances of data disclosure shall be recorded, and the traceability of data processing shall be ensured.

3.5. Data Subjects shall be afforded the rights laid down in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, subject to the exceptions provided therein.

4. Recipient of the request

4.1. Data shall be disclosed by the holder of the data relating to the relevant domain name - the Registry Operator for the .lv top-level domain or the Registrar managing the domain name.

4.2. The requester shall address the data disclosure request to the appropriate Registrar or the Registry Operator on the basis of the information available in the NIC Whois database.

5. General principles for the form and submission of requests

5.1. Requests shall be sufficiently detailed to identify the domain name, the law or regulation and the specific provision under which the requester is entitled to request and receive the particular personal data, as well as why the data are required and the purpose for which they will be used. Where applicable, documents substantiating the need to obtain the data shall be attached.

5.2. The request shall be made in writing, shall be legally valid and shall include information identifying the requester.
5.3. Data disclosure requests may be submitted to the Registry Operator for the .lv top-level domain in Latvian or English, and to .lv Registrars in the languages indicated by them.
5.4. Requests shall be accepted through the communication channels specified by the recipient of the request.

6. Verification of identity and compliance of the request

6.1. The recipient of the request shall have the right to verify the identity of the requester before assessing the legal basis for data disclosure.
6.2. Data shall not be disclosed where the identity of the requester cannot be verified, there is no sufficient legal basis for receiving the data, or another ground for refusing disclosure exists.

7. Review procedure and time limits

7.1. Requests shall be reviewed within the time limits prescribed by laws and regulations.
7.2. The decision to disclose data or refuse disclosure shall be documented and made on the basis of the requirements of laws and regulations and the principles laid down in the Disclosure Policy.

8. Other provisions

8.1. The Disclosure Policy shall be applied together with the Policy for acquisition of the right to use domain names under the top-level domain .lv, the NIC Privacy Policy, other rules of the Registry Operator published on its website, and applicable laws and regulations.
8.2. The Disclosure Policy shall not restrict the right of a Registrar to introduce more detailed procedures, provided that they comply with applicable laws and regulations and the Disclosure Policy.
8.3. The Disclosure Policy shall enter into force on 1 September 2026.
8.4. The Disclosure Policy may be reviewed and amended at any time, in which case the amended Disclosure Policy shall enter into force upon its publication on the website of the Registry Operator for the .lv top-level domain.
8.5. In the event of any conflict between the Disclosure Policy and the Policy for acquisition of the right to use domain names under the top-level domain .lv, the Policy for acquisition of the right to use domain names under the top-level domain .lv shall prevail.

---

[i] A botnet is a collection of devices (bots) infected with malware that operates under the commands of a botnet command-and-control (C&C) server. A botnet C&C server typically instructs members of the network to obtain information from their host systems or to carry out malicious activities, such as a distributed denial-of-service (DDoS) attack.

[ii] Malware is any software that, once installed, performs unwanted or malicious activities, often for the benefit of a third party. Adware, spyware and computer viruses are some of the best-known types of malware.

[iii] Pharming is a form of fraud in which an attacker redirects Internet users to a fraudulent website in order to steal their login credentials and other sensitive information. In a pharming attack, the attacker changes the IP address of a trusted domain name by hijacking the domain name registration or poisoning the cache of a name server (DNS server). The altered IP address redirects users to a website created by the attacker and disguised to appear to be the website of the legitimate Registrant. Once on the fraudulent website, users are deceived into entering their login credentials, credit card numbers or other sensitive information, which is then obtained by the attacker.

[iv] Phishing is a form of fraud in which an attacker impersonates a trusted person or organisation in order to infect a computer with malware or obtain sensitive information, such as a username, password or credit card details. Attackers often deceive victims by sending e-mails or other electronic messages that appear to originate from a trusted person or reputable organisation. Phishing messages usually contain a link directing the victim to a fraudulent website, where the victim is deceived into disclosing login credentials or other private information.

[v] Spam consists of unsolicited bulk electronic mail messages that the recipient has not consented to receive and that are sent as part of a wider messaging campaign in which all or most messages have substantially identical content. Put simply, spam is unsolicited e-mail sent simultaneously to a large number of recipients without their consent.