UTRDBA

DOMAIN REGISTRANT DATA COLLECTION, VERIFICATION, PUBLICATION AND DISCLOSURE POLICY

1. General

This policy defines the manner in which Utrdba d.o.o. (hereinafter: registrar) collects, verifies, uses, publishes and discloses data of domain holders (registrants) for domains it manages.

This policy applies to:

- national domains (e.g. .SI)
- generic domains (e.g. .COM, .NET, .ORG)
- regional domains (e.g. .EU)

For individual TLDs, additional rules of the competent registry may also apply.

2. Purpose of data collection

The registrar collects registrant data for the purpose of:

- identification of the domain holder
- ensuring technical functionality of the domain (DNS)
- enabling communication with the holder
- prevention of abuse (spam, phishing, malware)
- fulfillment of contractual and legal obligations
- cooperation with domain registries

3. Types of collected data

3.1 Basic data

- domain name
- registration / renewal date

3.2 Registrant data

- name and surname (natural person) or company name
- address (street, city, country)
- email
- phone number

3.3 Contact data (if separate)

- administrative contact
- technical contact

4. Method of data collection

Data is collected:

- upon domain registration
- upon domain renewal
- upon data modification
- upon domain transfer

The registrant guarantees the accuracy of the data and must report changes.

5. Data verification

The registrar performs data verification depending on the domain type.

5.1 Contact verification

At least one contact is verified:

- email (confirmation message)
- phone (format and reachability)

5.2 Identity verification (risk-based)

The registrar may verify identity:

- in case of suspected abuse
- at the request of the registry
- for high-risk domains

Possible methods:

- company verification (business registry)
- document identification
- payment verification

5.3 Periodic verification

- upon renewal
- upon abuse report
- at registry request

5.4 Failed verification

If verification fails:

- registrant is given a deadline (up to 21 days)

after which:

- domain may be temporarily deactivated
- or deleted

6. Public data (WHOIS / RDAP)

6.1 Legal entities

May be publicly visible:

- name
- country
- technical contact
- registrar

6.2 Natural persons

- personal data is hidden (GDPR)
- only email or anonymized contact may be shown

7. Disclosure to third parties

Data may be disclosed:

7.1 Upon legal request

- courts
- police

- authorities
- CERT/CSIRT

7.2 Upon legitimate interest

- trademark owners
- legal proceedings
- dispute resolution (UDRP / ARDS)

8. Data protection

Processing of personal data related to domain registration is carried out in accordance with the Privacy Policy of Utrdba d.o.o., which is publicly available on the company website.

9. Data retention

Data is stored:

- for the duration of the domain

After expiration:

- for legal requirements
- for dispute resolution

10. Responsibility of the registrant

The registrant:

- is responsible for data accuracy
- must keep data updated

- bears consequences of incorrect data

11. Registry specifics

The registrar acts as an intermediary and must comply with:

- Register.si rules for .SI
- ICANN rules for gTLDs
- EURid rules for .EU

12. Policy changes

The registrar may modify the policy due to:

- legislation
- registry requirements
- security reasons

Komenda, 19.3.2026