

Non-Public gTLD Registration Data Disclosure Policy

1. Purpose and Scope

This Policy establishes the procedures and requirements governing the submission, assessment and, where appropriate, disclosure of requests for non-public registration data relating to generic top-level domain names registered with Atak Domain Bilgi Teknolojileri A.Ş.

For the purposes of this Policy, Atak Domain Bilgi Teknolojileri A.Ş. is referred to as the “Registrar.”

This Policy has been prepared in consideration of Section 10 of the ICANN Registration Data Policy, the European Union General Data Protection Regulation (“GDPR”), the Turkish Personal Data Protection Law No. 6698 (“KVKK”) and other applicable laws and regulations.

2. Non-Public gTLD Registration Data

Non-public gTLD registration data means domain name registration data that is not publicly displayed and that may constitute personal data or confidential information.

Such data may include, without limitation:

- The Registered Name Holder’s first and last name,
- Organization or company information,
- Postal address,
- Telephone number,
- Email address,
- Administrative and technical contact information,
- Other non-public data elements relating to the domain name registration.

Registration data that is already publicly available, such as the domain name’s creation, update and expiration dates, is not treated as non-public registration data under this Policy.

3. Submission of a Disclosure Request

Requests for the disclosure of non-public gTLD registration data must be submitted in writing through one of the following channels:

- **Email:** hukuk@atakdomain.com
- **Support request:** A support ticket submitted through the Atak Domain customer or reseller control panel



For a request to be considered complete, the requestor must provide all of the information specified below.

3.1. Requestor's identity and contact information

The request must include:

- The requestor's full name or legal business name,
- Email address,
- Telephone number,
- Postal address,
- Contact information of any representative acting on behalf of the requestor.

The Registrar may request additional information or documentation to verify the requestor's identity and contact information.

3.2. Nature and type of the requestor

The requestor must identify the category under which the request is being made, including, as applicable:

- Individual,
- Private legal entity or commercial organization,
- Law firm or authorized representative,
- Intellectual property or trademark representative,
- Law enforcement authority,
- Court or judicial authority,
- Governmental or regulatory authority,
- Cybersecurity researcher or security organization,
- Other.

Where a request is submitted by an attorney, representative or other authorized person, evidence of the applicable authority or representation must be provided.

3.3. Relevant domain name

The request must clearly identify the gTLD domain name or domain names to which the request relates.

3.4. Requested data element values

The requestor must separately and specifically identify each non-public registration data element requested.

Requested data elements may include, for example:

- Registered Name Holder's first and last name,
- Organization or company name,
- Postal address,
- Email address,

- Telephone number,
- Administrative contact information,
- Technical contact information,
- Other specifically identified registration data elements.

General or unspecified requests for all available registration data may be returned to the requestor for clarification.

3.5. Purpose and legal basis of the request

The requestor must provide:

- The specific purpose of the request,
- The facts or circumstances giving rise to the request,
- The legal basis relied upon for disclosure,
- The requestor's legitimate interest, authority or legal entitlement,
- The connection between the request and the relevant domain name,
- Any supporting court order, official notice, investigation reference, trademark certificate or other relevant evidence.

3.6. Good-faith affirmation

The requestor must provide the following affirmation:

I affirm that this disclosure request is being made in good faith, that the information contained in the request is true and complete to the best of my knowledge, and that the request is not being made for an unlawful, misleading, abusive or unrelated purpose.

3.7. Agreement to process disclosed data lawfully

The requestor must provide the following agreement:

I agree that any registration data disclosed in response to this request will be processed solely for the stated purpose and in accordance with all applicable data protection laws and other legal obligations. I further agree not to disclose the data to unauthorized persons and to implement appropriate technical and organizational security measures.

4. Identity and Authority Verification

Depending on the nature of the request, the Registrar may require one or more of the following:

- Identification document,
- Company or organization registration document,
- Authorization document or power of attorney,
- Attorney or professional credential,
- Government-issued identification,
- Official correspondence,
- Court order,



- Investigation or case reference number,
- Trademark registration certificate,
- Other documentation supporting the request and its legal basis.

A request may be denied where the required documents are not provided or the requestor's identity or authority cannot be reasonably verified.

5. Acknowledgment of Receipt

The Registrar will acknowledge receipt of a Disclosure Request through the email address specified in the request or through the support ticket used to submit the request, as soon as reasonably practicable.

Where an initial review identifies missing mandatory information or documentation, the Registrar will notify the requestor of the missing items through the same communication channel.

The applicable review period begins when all required information and supporting documentation have been received by the Registrar.

6. Review Process and Response Time

A complete Disclosure Request will be assessed and the outcome communicated to the requestor no later than **five business days from receipt**.

Requests involving DNS abuse, an ongoing serious security threat, an imminent threat to human life, a court order or an urgent request from a competent authority will be prioritized. For such urgent requests, the Registrar aims to respond within **24 to 48 hours**, where reasonably practicable.

The review period may be extended where a request is complex, concerns multiple domain names, requires additional legal assessment or depends upon further information or documentation from the requestor. In such circumstances, the requestor will be informed of the reason for the delay and, where possible, the anticipated response time.

The review period may be suspended while the Registrar is awaiting required additional information or documentation from the requestor.

7. Assessment Criteria

Each Disclosure Request is assessed manually and on its individual merits.

The Registrar may consider, among other factors:

- Whether the requestor's identity and authority have been verified,
- Whether the request is clear, specific and complete,
- Whether the requested data element values have been specifically identified,
- Whether the requestor has demonstrated a valid legal basis or legitimate interest,
- Whether the requested data is necessary for the stated purpose,

- Whether the request has been submitted in good faith,
- The rights and freedoms of the Registered Name Holder,
- Whether the request appears abusive, fraudulent, harassing or unlawful,
- Whether disclosure would comply with the GDPR, KVKK and other applicable laws,
- Whether the request may be satisfied by disclosing a more limited set of data.

Submission of a request does not create an automatic entitlement to disclosure.

8. Decision on a Disclosure Request

Following its assessment, the Registrar may:

- Approve the request in full,
- Approve the request in part,
- Place the request on hold pending further information or documentation,
- Deny the request.

Any disclosure will be limited to the data element values that are necessary and proportionate for the substantiated purpose of the request.

9. Notification of the Decision

The Registrar's decision to approve, partially approve or deny a Disclosure Request will ordinarily be communicated in writing to the requestor's verified email address.

Where the request was submitted through the Atak Domain customer or reseller control panel, the decision may also be communicated through the relevant support ticket.

The decision notice will state:

- Whether the request has been approved, partially approved or denied,
- In the case of partial approval, which data elements will and will not be disclosed,
- In the case of denial, the reason for the denial to the extent that it may lawfully be provided,
- Any additional information or documentation required,
- Where the request is approved, the secure channel through which the data will be transmitted.

The requestor will be notified through the same verified email address or support ticket of the specific channel that will be used to transmit any approved data.

10. Means of Providing Disclosed Data

Where a Disclosure Request is approved, the relevant non-public registration data may be transmitted through one of the following secure methods, depending on the nature of the request and the status of the requestor:

- Delivery to a verified and designated email address,
- Password-protected attachment or encrypted email,

- Secure transmission through the Atak Domain support system,
- An official electronic correspondence channel used by a competent governmental authority,
- Another secure communication channel verified in advance by the parties.

The requestor will be informed in advance of the communication method that will be used.

Where a password-protected file is used, the password will, where reasonably practicable, be transmitted through a communication channel separate from the channel used to transmit the data.

The Registrar reserves the right not to disclose data through channels that it considers insecure or that do not permit adequate verification of the requestor's identity.

11. Grounds for Denial

A Disclosure Request may be denied in full or in part where:

- The requestor's identity or authority cannot be verified,
- Required information or documentation has not been provided,
- The requested data element values have not been specifically identified,
- No valid legal basis or legitimate interest has been demonstrated,
- The requested data is not necessary or proportionate for the stated purpose,
- The request is misleading, excessive, unrelated, abusive or made in bad faith,
- Disclosure would violate applicable data protection laws,
- Disclosure would have a disproportionate impact on the rights and freedoms of the Registered Name Holder,
- The supporting information or documentation is considered unreliable,
- The applicable retention period has expired or the requested data is not under the Registrar's control.

A denial decision will be communicated to the requestor through the verified email address or relevant support ticket.

12. Security and Confidentiality

Non-public registration data will only be disclosed to lawful, verified and authorized requestors.

Appropriate technical and organizational safeguards will be applied during the disclosure process.

Disclosure will be strictly limited to the data elements necessary for the specific request. Excessive or unrelated information will not be disclosed.

Where appropriate, the Registrar may mask, limit or redact certain data elements before disclosure.

13. Record Keeping

The Registrar may maintain records relating to Disclosure Requests, including:

- Date of receipt,
- Requestor's identity and contact information,
- Relevant domain name,
- Requested data element values,
- Purpose and legal basis of the request,
- Supporting documentation,
- Assessment undertaken,
- Decision issued,
- Data element values disclosed,
- Dates of the decision and disclosure,
- Communication channels used.

Such records will be retained only for compliance, audit, security, legal obligation and dispute-resolution purposes, in accordance with applicable laws and ICANN requirements.

14. Implementation and Audit

The implementation of this Policy will be monitored regularly by Atak Domain Bilgi Teknolojileri A.Ş.

Procedures for receiving, assessing, responding to and recording Disclosure Requests may be subject to internal compliance reviews and audits.

The Registrar may provide relevant records and information in connection with ICANN audits or lawful requests from competent authorities.

15. Legal Basis

This Policy has been prepared in accordance with:

- The ICANN Registration Data Policy, particularly Section 10,
- The European Union General Data Protection Regulation,
- The Turkish Personal Data Protection Law No. 6698,
- Other applicable national and international laws and regulations.

16. Amendments and Updates

This Policy may be amended in response to changes in ICANN policies, applicable data protection laws or the Registrar's operational procedures.

The current version of the Policy will be published on the Atak Domain website.