

Domain Name Registration Data Policy

Easyhost bv – Verification, publication and disclosure of domain name registration data (Article 28 NIS2)

1. Scope

Easyhost bv, with registered office at Skaldenstraat 121, 9042 Ghent, Belgium, company number BE 0455.977.006 (hereinafter: "Easyhost" or "we"), provides domain name registration services, either as an accredited registrar or as a reseller of an upstream registrar.

This policy describes how we ensure accurate and complete registration data, how we publish this data, and under what conditions we disclose it, in accordance with Article 28 of Directive (EU) 2022/2555 (NIS2) and the Belgian Act of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public security.

This policy applies to all domain names we manage, regardless of the top-level domain (TLD) concerned.

2. Registration data

We collect and keep the following data in a dedicated database: the domain name, the registration date, the name, email address and telephone number of the domain name holder and, if different, the email address and telephone number of the point of contact responsible for managing the domain name. We also record whether the domain name holder is a natural person or a legal entity.

Registries may require additional data.

Domain name holders must provide accurate data and keep it up to date via <https://my.easyhost.be>.

3. Verification

Verification is carried out on our behalf through a central verification system managed by team.blue NV, as well as by registries or registrar suppliers. The same procedure applies to all domain names we manage. The depth of the verification depends on the rules of the registry concerned and on the assessed risk of the registration.

3.1 Verification levels

- **Validation:** each data element is automatically checked for completeness, correct format and consistency, for example the syntax of an email address or the international format of a telephone number. Data that does not pass validation is not forwarded to the registry.
- **Contact data verification:** we confirm that a communication channel exists, is active and reaches the domain name holder.
- **Identity verification:** we confirm that the domain name holder is the person or organisation they claim to be.

3.2 When we verify

Event

What we do

Registration	Validation, risk assessment and the verifications required for the domain name, before or shortly after the registration of the domain name.
Change of domain name holder or contact data	The requester is authenticated, the new data is validated and, where it concerns a previously verified data element or a new domain name holder, verified again.
Transfer to Easyhost	The registration data is verified, unless an existing verification can be reused.
Transfer away from Easyhost	The transfer is not hindered by the verification procedure.
Reporting of inaccurate data	Reports of inaccuracies, reports of abuse and notifications from registries or competent authorities are investigated and may lead to a new verification.

3.3 Risk assessment

Every registration is subject to an automated risk assessment of the domain name. This evaluates linguistic, structural and reputation-related indicators, such as similarities with existing domain names or trademarks, patterns characteristic of automatically generated names, and links to known malicious activity.

Where the assessment indicates an elevated risk, identity verification is required. No other personal data is used for the risk assessment.

3.4 Methods

Check		When	Method
Email address	Always		A link containing a one-time code is sent to the email address. The code is valid for a limited period and for a limited number of attempts.
Telephone number		When the registry requires it	A one-time code by SMS or voice call, at the domain name holder's choice.
Identity		When the risk assessment indicates an elevated risk, or when a registry or competent authority requires it	Verification of the authenticity and validity of an official identity document on a page managed by our verification provider.

No biometric data is processed.

3.5 Reuse of verifications

A successful verification may be reused for the same person and the same data within the validity period set by the applicable rules. A new verification is required once that validity period has expired or when the data has changed.

3.6 Registries and upstream registrars

Where a registry or our upstream registrar carries out a verification itself, we do not collect the same data again. We guide the domain name holder through that procedure and ensure that our data remains aligned with its outcome.

Where a registry requires the verification status to be reported, we report that status.

3.7 Failed verification

Domain name holders are informed of the required verification and of the consequences if they do not complete it. If the verification is not completed, the domain name may be suspended, deleted, or subjected to

both measures.

For active domain names, we notify the domain name holder and set a deadline to remedy the deficiency. After that deadline has passed, the domain name may be suspended or deleted.

Immediate measures may be taken where required by law or by an imminent risk of abuse. Stricter rules of the registry concerned take precedence.

3.8 Proof of verification

Each verification results in a record of its outcome, method, time and scope. On request, we provide this proof to registries, our upstream registrar or competent authorities.

4. Publication

Without undue delay after registration, we make the registration data that does not constitute personal data publicly available through the registry's registration directory service.

For legal entities, this includes the name, telephone number and email address of the domain name holder.

Data of natural persons is not published, unless the rules of the registry concerned require it and a valid legal basis exists for doing so.

5. Access for legitimate access seekers

Legitimate access seekers, such as competent authorities, law enforcement agencies and CSIRTs, may request access to registration data that is not publicly available.

Requests must be submitted via data.protection@easyhost.be and must state the identity of the requester, their legal capacity, the domain name concerned, the data requested, the purpose of the request and the legal basis.

We assess each request in accordance with the applicable data protection legislation and respond without undue delay and in any event within 72 hours of receipt. We provide the data in full or in part, or refuse the request with reasons.

The data is transferred via a secure channel.

6. Data protection and contact

More information about the processing of personal data in the context of the verification procedure, including information about service providers, retention periods and your rights, is included in our privacy policy: <https://www.easyhost.be/en/privacy-policy>.

Questions about this policy can be addressed to: data.protection@Easyhostgroup.com.

Version

Current version: **26/10/2026**