Approved on 5 December 2022 by the decision of the Board of the Estonian Internet Foundation

In force from 1 January 2023

EIF PRINCIPLES FOR THE MANAGEMENT OF CONTENT ON THE ESTONIAN INTERNET

The main activity of the Estonian Internet Foundation is the management, development, and security of the infrastructure (i.e., DNS) of the .ee Top Level Domain (TLD) and the organisation of domain name registration. In carrying out its tasks, the Estonian Internet Foundation (EIF) is guided by the values of a cleaner, fairer, and safer Internet. The .ee domain name registry managed by the EIF stands out in terms of the security of its zone, which is ensured in particular through the electronic identification of registrants and the verification of the data submitted.

At the same time, we can also find a variety of malicious content in the secure .ee zone, where the EIF must contribute to the purity and integrity of the Internet. Due to the EIF's position as the administrator of the .ee infrastructure and registry, the EIF has the technical capacity to stop the display of content related to .ee domain names and the proliferation of infringements on the Internet, as well as to implement notations concerning prohibition on .ee domains.

1. INFRINGEMENTS AND MALICIOUS BEHAVIOUR

Malicious activities or infringements on the Internet can be divided into two categories:

1.1. Infringements related to website content
1.2. Infringements of a technical nature

The following list of examples illustrates the infringements related to website content:

- Products and services designed to deceive consumers (e.g., in e-shops)
- Illegal sale of goods – e.g., medicines, drugs, weapons, stolen goods
- Extremist content – e.g., incitement to terrorism, extreme depictions of violence
- Content related to the sexual exploitation of minors
- Hate speech/defamation – racial, religious, or ethnic discrimination, violence or threats
- Intellectual property infringements – counterfeiting, infringement of a patent or trade secret, piracy, unauthorised use of a trademark (not including the domain name itself)
- and other content that is incompatible with the law of the Republic of Estonia or the EU.

Infringements of a technical nature are generally:

- Infecting with malware
- Spamming
- Phishing
- Pharming

2. EIF's OPPORTUNITIES IN CONTENT MANAGEMENT

In the case of these infringements and malicious practices, the EIF is in a position to take various measures to ensure a safer and cleaner Internet for all. Measures that can be taken by the Estonian Internet Foundation to eliminate infringements:

- Disclosing the registrant's details to the entitled person
- Contacting the registrar
- Applying notations concerning prohibition
- Suspending domain name registration
- Deleting the registration and adding the domain name to the blocked/reserved list

3. IMPLEMENTATION OF EIF MEASURES

The first criterion for the application of a measure is the fact of the occurrence of an infringement. In general, the EIF relies on notifications or injunctions issued by the competent authority (see the next chapter on the competent authority). If a third party has submitted a report or observation, the EIF will normally refer it to the competent authority which will assess whether an infringement has taken place and the extent and impact of the infringement.

In the case of an injunction issued by a competent authority, the EIF will implement the measure referred to in the injunction issued by the entitled person, by checking the legal basis of the claim by the third party and explaining the consequences of the measure.

In the case of a notification or observation by a competent authority, the EIF will assess the extent and impact of the infringement based on its expertise and will independently take an informed decision to impose restrictions on the domain name.

In making its informed decision, the EIF will consider each case on its own merits and will base its decision to suspend a domain name on the proportionality between the infringement and the consequence. In particular, the suspension or deletion of a domain name registration to address the infringement must be a last resort to remove the infringement from the Internet. The EIF will check whether the person has previously exhausted all avenues to remedy the infringement by other means, including contacting the registrant, the online service provider and the registrar.
For example, if one ad on a popular advertising portal is disturbing, it is not proportionate to suspend the domain name registration and thus the website entirely. In this case, the right thing to do would be to contact the administrator of the website or the web server provider and ask them to remove the ad. If this is unsuccessful and the infringement has been assessed to be sufficiently serious, the domain name should only be suspended or deleted as a last resort to remove the content.

Although the EIF has the capacity to suspend the registration of an .ee domain name, as a result of which the content of a website hosted under the domain name becomes unavailable to Internet users, suspending the registration of a domain name is a severe infringement of the registrant's rights. At stake here are two very important values of our society – freedom of expression and enterprise on the one hand, and social security on the other.

In today's world, the Internet is the most accessible and influential place to exercise one's freedom of expression and enterprise, so domain registration suspension should be a last resort for restricting online content – in the first instance, the registrant, the web server provider or the registrar will be contacted directly to remove specific information (e.g. a disturbing image, a false news story, etc.) presented via the web interface. Only as a last resort will the EIF suspend the registration of an .ee domain name, which in turn will also suspend the display of content hosted there.

The EIF is protecting and will always protect the interests of registrants vis-à-vis third parties, i.e. before an entitled third party seeks to impose a restriction on a domain name, the EIF will seek to clarify the consequences of that action and how it will affect the domain name registrant and our freedoms in general.

4. EIF's PARTNERS IN CONTENT MANAGEMENT

The EIF works with third parties to ensure the security and purity of the .ee zone content. In deciding on the infringement and removing the content, the EIF generally relies on the notification or injunction given by a downstream partner.

- Consumer Protection and Technical Regulatory Authority
- Police and Border Guard Board
- Financial Intelligence Unit
- CERT-EE (Information System Authority)
- Estonian Internal Security Service
- Court
- Prosecutor's Office
- .ee accredited registrars

Here are some examples of what and on which basis the different authorities in Estonia are currently involved in the management of online content and who to contact in which cases:

It is worth contacting the Consumer Protection and Technical Regulatory Authority in cases involving the protection of consumer rights and misleading content. Under the Consumer Protection Act, the Consumer Protection and Technical Regulatory Authority has the power to require the EIF to block access to the domain or to delete the registration of the domain name referred to in the injunction if this is necessary to protect consumer rights. Also, under the Media Services Act, the Consumer Protection and Technical Regulatory Authority has the right to block access to domestic .ee domain names as well as to other top-level domain names (geo-blocking) if they violate the requirements set out in the Media Services Act. Under Regulation (EU) 2021/784, the Consumer Protection and Technical Regulatory Authority has the power to require an online service provider to remove terrorist content. Similarly, if you see terrorist content on the Internet, the Estonian Internal Security Service is the authority to contact.

Contacts of the Consumer Protection and Technical Regulatory Authority
e-mail: info@ttja.ee
phone: +372 667 2000

Contacts of the Estonian Internal Security Service
e-mail: kapo@kapo.ee
phone: +372 612 1455

CERT-EE is primarily responsible for detecting and responding to infringements of a technical nature. They can be contacted if you suspect a technical infringement.

Contacts of CERT-EE
e-mail: cert@cert.ee
phone: 663 0299

The Police and Border Guard Board and the courts should be contacted if you suspect an infringement of intellectual property – we strongly recommend that you seek legal advice in these cases. The Police and Border Guard Board and the courts also have the competence to settle disputes related to hate speech and defamation. The Police and Border Guard Board is also the right place to contact if a crime has been committed via the Internet.

Contacts of the Police and Border Guard Board
e-mail: ppa@politsei.ee
phone: 612 3000

The EIF has also signed cooperation agreements with the Police and Border Guard Board and CERT-EE for preventive action, whereby the respective authorities have access to domain name data to prevent and deter malicious activity and to quickly identify registrant details.

The EIF publishes a periodic overview of the number of times the EIF has had to intervene based on an injunction or a request and the reasons and justifications for removing content from the Internet.

The EIF can be contacted for all of the above – we will provide explanations and, where necessary, refer you to the right place to make the Internet safer and cleaner.

If you discover or suspect an infringement, please let us know by sending an e-mail to info@internet.ee.

ANNEXES

1. List of domain names currently subject to restrictions.
2. A periodic overview of how many times the EIF has intervened on the basis of injunctions or requests and the reasons for doing so.