Requests Policy

[For competent authorities]

In order for our company to be able to better assist law enforcement agencies and/or other regulators we have established a system to ensure any such requests are handled efficiently and without delay.

The processing of requests, of competent authorities, for the purpose of providing responses, is subject to this policy with specific terms and conditions (hereinafter "Policy" or "Requests Policy"). The Policy outlines the provisions and the predefined procedures after which EasyBit (hereinafter referred to as "we", "us" or "Service") provides responses to such requests in relation to easybit.com (hereinafter "Website" or "Platform") and any associated services.

Table of Contents

1. Competent Authority

As competent authority is defined, any party, person, or organization, that is legally empowered by the government, state, municipality, or similar, to exercise or perform the powers, duties, and functions of filing requests for obtaining information or conducting investigations and may extend to security forces; competent governmental, intergovernmental or supranational bodies; competent agencies, departments, regulatory authorities, self-regulatory authorities or organizations.

2. Terms and Conditions

2.1 Documentation Terms and Conditions

In our effort to assist any such Competent Authority effectively and promptly EasyBit shall require documentation supporting the request.

The documentation supporting the request for information (hereinafter "Information Request") should contain what is specified in this section and shall be created and sent to us in accordance with this Policy.

- Shall be made on a legal basis;
- Shall be issued by a competent authority, as defined in Section 1. with the legal power to request and process such information;
- Shall include complete, accurate, and valid information about the competent authority issuing the request;
- Shall include a postal address, contact phone numbers, and website, if any, of the competent authority;
- Shall include an official email address associated with the competent authority in question, in which we will provide our response;

- Shall be shared with us from an official email address associated with the competent authority;
- Shall be made in, or translated to, English;
- Shall be signed and stamped;
- Shall include the full name and title of the person in charge of the inquiry;
- If any person, different from the person in charge of the inquiry, will receive the information on his/her behalf, a relevant authorization shall be included along with the full name and identification information of the receiver;
- Shall contain a description of the type of information that the competent authority wishes to receive.

In addition, any information relevant to the request should be included in great detail, e.g. if the request is in regard to a transaction, such information as involved wallet addresses, transaction hash, and amounts transferred, along with any other transaction details available and relevant important information should be included, in order for our team to be able to process the inquiry in the most efficient way.

The Information Request may be directed to our legal department at the following email address: legal@easybit.com.

EasyBit, will take all necessary actions to ensure the security and confidentiality of all information and documents provided by the competent authority.

Upon our review of the above, we may choose to reply with any information at our disposal in association with the Information Request (hereinafter "Information").

2.2 Information Terms and Conditions

By forwarding an Information Request to us, you accept the Terms in this Policy and you declare and warrant that:

- You represent a competent authority as defined in Section 1.;

- You are legally empowered in your jurisdiction to request such information;
- The use of the Information will be legal at all times and in association with the purposes of the Competent Authority issuing the Information Request;
- You are not furthering, performing, undertaking, engaging in, or aiding any unlawful activity through the information you request to receive;
- You are responsible to maintain such information for as much as provisioned by applicable laws;
- You are responsible to safeguard such information and take organized efforts in the direction of avoiding any data leakage.

3. Processing of Requests

All Information Requests undergo thorough reviewing, verification, and processing. Such procedures usually last 5 to 10 business days, but on certain occasions might take longer in accordance with service load and the complexity of the request.

As a first step, EasyBit will review all provided documentation and information to ascertain the authenticity of the information request, to verify that the authority issuing it is indeed empowered to exercise or perform the duty of filing such information requests, to ensure that such request would be in accordance with applicable laws, and/or to verify the identity of the parties involved if deemed necessary.

On certain occasions and types of requests or when the above-mentioned are not verified, EasyBit may come back with more requirements, extra measures, or certain procedures that might be considered essential. Instances of extra requirements include but are not limited to, extended identification procedures, and the documents to be enforced and recognized in our own jurisdiction, among others.

If the received Information Request is incomplete EasyBit may revert and request further information and/or documentation from the Competent Authority filing the Information Request.

After the reviewing and verification procedures are successfully completed, EasyBit will process the inquiry and take all necessary actions to satisfy it in the most efficient way.

Should any of our efforts yield results - we will respond accordingly to the competent authority's email address with any findings.

4. AML Procedures

We maintain AML systems and procedures which may be triggered following an Information Request by a competent authority.

Part of these procedures is our blacklisting policy after which we blacklist all data ever kept by our systems, relating to the user(s) that we were informed may be involved in illegal activities. Additionally, our blacklisting policy may contain KYC requirements for the said user(s). The user will not be made aware that restrictions are in place against him/her, as the KYC procedure will be conducted normally and as provisioned by our AML System. For more information about the AML System and the relevant procedures please refer to our AML Policy.

Finally, we respect and applaud the efforts of any investigating body and do our best to collaborate with them and assist them in the direction of fighting organized crime and unlawful activities and remain committed to assisting in any way possible.

5. Limitation of Liabilities

EasyBit takes all necessary actions and measures, uses the best available practices, and the most efficient course of action in order to satisfy any legitimate request and provide the competent authorities with the information requested. All information is provided on an ‘‘as is” and ‘‘as available” basis. In no event shall EasyBit, the owner, our directors, officers, members, or any kind of employees or agents be liable or responsible, for the accuracy, adequacy, and completeness of the disclosed information provided in response to the relevant request by the competent authority, and exempts liability for deficiency or errors that may arise as a result of human error or email transmission.

Any provided information distributed to the competent authority through email correspondence shall be deemed privileged and confidential and shall be used only for the purposes of the request. Any unauthorized use, reproduction, or dissemination of the email correspondence and its attached documents, if any, is strictly prohibited. Any third party falsely claiming to be and/or impersonating a Competent Authority may face criminal liability and/or prosecution.