PRIVACY POLICY

General information and definitions:

Company and data controller:	**Husky Fintech OÜ.** Registered in Estonia with registration number: 14927539.
Address:	Harju maakond, Tallinn, Haabersti linnaosa, Meistri tn 16-401, 13517
License(s):	FVT000246 - Providing a virtual currency service (services of exchanging a virtual currency against a fiat currency, a virtual currency wallet service). Both licenses were provided in Estonia.
Website/Platform	A website that is operated by the Company and available at https://broex.io/
Customer	An individual Customer from an age of 18+ or a legal entity that has read and agreed to the Customer Agreement of Company and uses services of the Company provided through the Website Platform.
Personal data	Any information relating to Customer, which identifies or may identify a Customer and which includes such data like Customer's name, address and identification number.
GDPR	The General Data Protection Regulation (EU) 2016/679.

KYC or Due Diligence	Documents that are requested by Company from the Customers in order to identify the Customer and comply with applicable laws.
Last updated	01 June 2021

Purpose

The Privacy Policy is meant for use by Customers of Company.

The company is compliant with the applicable Estonian and International laws for the Prevention of Money Laundering and Terrorist Financing, the GDPR as well as repealing Directive 95/46/WE (general regulation on data protection) and other relevant binding provisions of law applicable in Estonia.

This Privacy Policy aims to provide Company's Customers with information on what type of information Company collects, how it is used and the circumstances where it could be shared with third parties.

Personal data

The Company shall collect information necessary to fulfil legal obligations for the provision of services and to improve Company services.

The Company may obtain Customer Personal Data from Customer directly (especially through the websites and/or online forms); and/or from third parties, service providers that are assisting Company in providing services and help Company to offer services effectively.

Customer's Personal data will be used for specific, explicit and legitimate purposes according to the Estonian and International laws for the Prevention of Money Laundering and Terrorist Financing, as well as in order to enhance Customer support.

The Personal data collected from Customers is used to verify Customer's identity for Due Diligence purposes, to manage Customer's account with the Website Platform, to process Customer's transactions, to provide Customers with post-transaction information, to inform Customers of additional products and/or services relevant to Customer's profile, to produce analysis and statistical data which will help the Company improve its products and services, and also for the Website Platform enhancement purposes.

Company may collect the following Personal Data:

- information such as name, surname, nickname, email, address and other information that are necessary to identify Customer and to prevent using account by unauthorized parties;
- data about Customer account (we may create a specific ID for you when you use the Services);
- IP address and unique mobile device identification numbers (such as Customer device ID, advertising ID, MAC address);
- data about Customer device, such as manufacturer, operating system, CPU,

RAM, browser type and language;
- broad location data (e.g. country or city-level location);
- precise geolocation data (GPS);
- data (such as Customer nickname, profile picture) received if Customer link a third-party tool with the Service (such as Facebook, Google, etc.);
- details of orders (amount spent, date, time, vouchers or offers used);
- data collected with cookies and similar technologies;
- data to fight fraud and data required by anti-money-laundering provisions;
- payment data (such as to verify payment);
- data for analytics purposes, so can provide Customer with a better service and/or other not used services;
- Customer messages and feedback about experience with Company;
- other Personal data Customer have sent.

Identity verification

The Company needs to perform its Due Diligence measures and apply the principles of KYC (Know-Customer's-Customer) before entering a business relationship with any Customer in order to prevent actions, such as money laundering or terrorist financing, and to perform other duties imposed by law.

Company collects from its Customers' identity verification information (such as copies, images, scans of Customer's government issued national ID card or International Passport, or other governmental proof of identification) or other authentication information. Company also requests its Customers to provide additional documents due to its AML Policy. Further to this, the Company can use third parties to carry out identity checks on its behalf.

Collecting and processing

Company and any third parties acting on Company's behalf for the purpose of collecting, storing and processing personal data may collect, process and store personal data provided by the Customer.

For the purpose of processing and the storage of personal data provided by the Customer in any jurisdiction within the European Union or outside of the European Union, the company can confirm this will be done in accordance with applicable laws.

Safeguarding legitimate interests

Company processes personal data to safeguard the legitimate interests pursued by Company or by a third party. A legitimate interest is when Company has a business or commercial reason to use Customer's Personal data. Even then, it must not unfairly go against what is right and best for the Customer.

Examples of such processing activities include:

- initiating court proceedings and preparing defense in litigation procedures;
- means and processes to provide for the Company's IT and system security, preventing potential crime, asset security, admittance controls and anti-trespassing measures;
- measures to manage business and for further developing products and services;
- the transfer, assignment and/or sale to one or more persons and/or charge and/or encumbrance over, any or all of the Company's benefits, rights, title or interest under any agreement between the Customer and the Company.

Marketing Purposes

The Company may process Customer's Personal data, such as location or transaction history to deliver any news (inform Customers about products, services), analysis, research, reports, campaigns and training opportunities that may interest the Customer, to their registered email address.

The Personal data that Company processes for this purpose consists of information Customers provide to the Company and data Company collects and/or infers when Customer uses services of the Website Platform, such as information on Customer's transactions. Company studies all such information to form a view on what is needed or what may be of an interest to Customers.

In some cases, profiling may be used. Profiling is a process when Customer's data is being automatically processed with the aim of evaluating certain personal aspects and to further provide Customers with targeted marketing information on services.

Customer always has the right to change the option if no longer wishes to receive marketing related emails to Customer's provided email address.

Customers have the right to object at any time to the processing of Customer's Personal data for marketing purposes or unsubscribe to the provision of marketing related emails by the Company, by contacting at any time Company's Customer support department via the following ways:

1. By Email: support@broex.io

2. Customer support via the Website Platform

Authorized Processor

The GDPR sets out what needs to be included in the contract which the Company has adhered to, obligations of all relevant parties, for example, are:

- third parties must only act on the written instructions of the Company (unless required by law to act without such instructions);
- ensure that processing the Personal data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- the rights of Customers will not be impaired in meeting with GDPR requirements;
- the security of processing, the notification of Personal data breaches and Personal data protection impact assessments will not be impaired;
- deletion or return of all Personal data as requested at the end of the contract.

Company has a regulatory obligation to supervise and effectively oversee the outsourced functions and to act appropriately when it determines that the service provider is not performing the said functions effectively and in accordance with the applicable legislation.

Company may use or disclose Personal data without Customer's consent only in certain circumstances:

- if required by law or by order of a court, administrative agency, or other government entities;
- if there are reasonable grounds showing disclosure is necessary to protect the rights, privacy, property, or safety of Customers or others;
- if believe the Personal data is related to a breach of an agreement or violation of the law, that has been, is being, or is about to be committed;
- if it is necessary for fraud protection, risk reduction, or the establishment or collection of funds owed to us;
- if it is necessary to enforce or apply the Terms and Conditions and other agreements, to pursue remedies, or to limit damages to Company;
- for other reasons allowed or required by law;
- if the Personal data is public.

When the Company is required or permitted to disclose personal data without consent, Company will not disclose more Personal data than necessary to fulfil the disclosure purpose.

Company informs all Customers to maintain confidentially and not to share with others its Customer names and private passwords or as provided by the Company. The Company bears no responsibility for any unlawful or unauthorized use of Customers' Personal data due to the misuse or misplacement of Customers' access codes (i.e. passwords/credentials), negligent or malicious, however conducted.

Period of keeping Customer's Personal data

The Company will keep Customer's personal data for:

- as long as a business relationship exists with the Customer;
- once the business relationship with Customers has ended, Company is required to keep Customer's Personal data for a period of five years to meet regulatory and legal requirements. In some cases, this period may be extended.

When Company no longer needs Customer's Personal data, Company will securely delete or destroy it.

Customer's rights

Customer has the right to request copies of his/her Personal data. Information of Personal data must be provided without delay and at the latest within one month of receipt. The Company will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, Company will inform Customers within one month of the receipt of the request and explain why the extension is necessary.

Company must provide a copy of the information free of charge. However, the Company can charge a "reasonable fee" when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The fee if applied will be based on the administrative cost of providing the information and for delivery expenses, if Customer requests to deliver this information in hard copy. If at any time Company refuse to respond to a request, Company will explain why to the Customer, informing Customer of their right to complaint to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Age policy

Company services are not directed to people younger than eighteen (18) years of age. Company do not intend to collect Personal data from such people. If you are under 18, please do not use the Services and do not send any Personal data about yourself to Company. In the event that Company learn that have collected Personal data from a person under age 18, will delete that Personal data as quickly as possible.

The Geographical Area of Processing

As a general rule, the Customer data is processed within the European Union/European Economic Area (EU/EEA), but in some cases it is transferred to and processed in countries outside the EU/EEA.

The transfer and processing of Customer data outside the EU/EEA can take place provided there are appropriate safeguards in place and the actions are made based on a legal basis only.

Upon request, the Customer may receive further details on Customer Personal data transfers to countries outside the EU/EEA.

Other information

Company uses appropriate technical, organizational and administrative security measures to

protect any Personal data and other information it holds in its records from loss, misuse, and unauthorized access, disclosure, alteration and destruction. Unfortunately, no company or service can guarantee complete security. Unauthorized entry or use, hardware or software failure, and other factors, may compromise the security of Customer Personal data at any time.

Among other practices, Customer's account is protected by a password for Customer's privacy and security. Customers must prevent unauthorized access to Customer's account and Personal data by selecting and protecting Customer's password appropriately and limiting access to Customer's computer or device and browser by signing off after finished accessing Customer's account.

Transmission of Personal data and information via regular email exchange is not always completely secure. The Company however exercises all possible actions to protect Customers' Personal data, yet it cannot guarantee the security of Customer data that is transmitted via email; any transmission is at the Customers' own risk. Once the Company has received the Customer Personal data it will use procedures and security features in an attempt to prevent unauthorized access.

When Customers email the Company or using the Contact form feature, a Customer may be requested to provide some additional Personal data, like their name or email address. Such data will be used to respond to query and verify Customer's identity. Emails are stored on Company's standard internal contact systems which are secure and cannot be accessed by unauthorized external parties.

Complaints

Any concerns and/or requests can be send:

Email: support@broex.io

Customer has the right to be confident that Company handles Customer's Personal data responsibly and in line with good practice.

If a Customer has a concern about the way the Company is handling Customer's Personal data, or for example if a Customer feels we may not be;

- keeping Customer's Personal data secure;
- holds inaccurate Personal data;
- has disclosed Personal data;
- is keeping Personal data about Customer for longer than is necessary;
- has collected Personal data for one reason and is using it for something else.

Company take all concerns seriously and will work with Customer to resolve any such concerns.

Customers written request may be required for security reasons. We may decline the request, if there are reasonable grounds to believe that the request is fraudulent, unfeasible or may jeopardize privacy of others.

If the Customer is not satisfied with any responses provided by the Company, the Customer has a right to raise such matters with the Estonian Data Protection Inspectorate:

- E-mail address: info@aki.ee
- 39 Tatari St., 10134 Tallinn, Estonia
- Phone: +372 627 4135

The Customer has the right go to court or to escalate complaint to the data protection regulator in their jurisdiction for the protection of rights, unless the applicable laws prescribe a different procedure for handling such claims.

Changes in Privacy Policy, review

The Company reserves the right to modify or amend this Privacy Policy unilaterally at any

The Company reserves the right to modify or amend this Privacy Policy unilaterally at any time in accordance with this provision.

If any changes are made, Company shall notify Customer accordingly. Company encourage Customer to review this Privacy policy occasionally so as to always be informed about how Company are processing and protecting Customer's Personal data.
The Company will review the Privacy Policy at least annually. A review will also be carried out whenever a material change occurs that affects the ability of the Company to continue to the best possible result for the execution of its Customer Orders on a consistent basis using the venues included in this Privacy Policy.

The Company will inform its Customers of any material change to this Privacy Policy by posting an updated version of this Privacy Policy on its Website and/or to Customer email.