

PRIVACY POLICY

INTRODUCTION

At **OÜ NeuronEX Platform** (hereinafter -“**Company**“, “**we**“, “**us**“, or “**our**”), we are committed to process, protect and respect your privacy according to the rules of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter – “**GDPR**”) and other applicable data protection regulations. This Privacy policy sets out key information regarding Company and how any personal data you provide to us will be processed and disclosed.

This notice also informs you about:

- How and what kind of personal data we collect and process;
- The purposes and legal basis for your personal data processing;
- The possible recipients or categories of recipients of your personal data;
- Personal data storage and retention;
- Your rights as data subject regarding your personal data;
- Other relevant information that we shall provide to you according to GDPR.

We recognize that personal data privacy is an ongoing responsibility, and so we may update from time to time this Privacy policy as we undertake new personal data practices or adopt new privacy policies.

For all other information regarding our services, please refer to our Terms & Conditions (Agreement).

Definitions and Key Terms defined in the Terms & Conditions of Company shall apply also to this Privacy policy.

NAME AND ADDRESS OF THE CONTROLLER

OÜ NeuronEX Platform is the controller and responsible for your personal

data. Name: **OÜ NeuronEX Platform**

Legal address: Harju maakond, Tallinn, Nõmme linnaosa, Kalda tn 9a, 11625, Estonia

Company Registry Code: 14917854

Email: support@neuronex.io

Neuronex.io website is owned and run by **OÜ NeuronEX Platform**.

For all questions relating to your private information or this Privacy policy, please contact us at support@neuronex.io.

MINORS

The website is not intended for minors and we do not collect personal data relating to minors.

If the Company recognizes that the Company has collected personal data from a child, Company will delete that information as quickly as possible. If you suspect that a child under 13 may have provided personal data to us, please contact us via e-mail: support@neuronex.io.

LEGAL BASIS APPLICABLE TO COLLECTION AND PROCESSING OF YOUR PERSONAL DATA

We collect and process your personal data in accordance with the rules of personal data processing and protection provided by GDPR and other applicable personal data protection legislation.

We may collect and process your personal data, based on one or several of the following legal grounds:

- (a) your consent to the personal data processing (*Article 6 (a) of GDPR*);
- (b) the performance of contractual or pre-contractual obligations with you (*Article 6 (b) of GDPR*);
- (c) compliance with the legal obligations, including Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (hereinafter – “**Regulation (EU) 2015/847**”) and Money Laundering and Terrorist Financing Prevention legislation (*Article 6 (c) of GDPR*);
- (d) legitimate interests (*Article 6 (f) of GDPR*).

Personal data types we may process, sources, purposes and justification for personal data processing

We may collect information about you when you visit our website or use our services, including the following:

REGISTRATION AND ACCOUNT OPENING

When you register to use our services by establishing an Account, we will collect your **email address and telephone number**. This is the minimum necessary for us in order to enter into a contractual relationship with you. As you continue to use our services, and your transactions exceed Euro 1,000 in a month, we will require additional information and documents for the purpose of verifying your identity and to comply with Know-Your-Client ("KYC"), Anti-money Laundering (“AML”) and Counter Terrorist Financing (“CTF”) procedures requiring Customers due diligence. These documents may include, but are not limited to the following personal data: your name, surname, personal identification number, address, information contained in Digitized copy of the ID/Passport, Utility Bill and Transaction data, which you submit to us according to these AML/KYC requirements.

The legal bases for collecting and processing of personal data as indicated above are: your consent, entering into and the performance of our contract with you, and our legal obligation to comply with the Regulation (EU) 2015/847 and Money Laundering and Terrorist Financing Prevention legislation.

TRANSACTION INFORMATION

When you use our services, access our website to make Cryptocurrencies exchange, we collect **personal data about the parties to the transaction** which may include some or all of the following: bank/payment institution account or other payment information, credit/debit card information (card number, CVC or CVV, card expire date, card holder Name and Surname) amounts sent and received, amounts paid for services.

Transaction data includes also details about:

- the type of Cryptocurrency involved, the order volume, price, value;
- your Cryptocurrency buy/sell Transactions records;
- transaction history, including withdrawals and Cryptocurrency and Fiat money exchanges;
- amounts credited to your Account and your Account balances.

The legal bases for collecting and processing of personal data indicated above are: the performance of our contract with you and our legal obligation to comply with the Regulation (EU) 2015/847 and Money Laundering and Terrorist Financing Prevention legislation.

LOGGING IN TO OUR WEBSITE (SITE)

If you have registered for an Account on our Site, we collect:

- **Technical/LOG Data** includes the IP address, your login data to the System (username and password), device type, browser type, time zone setting and location, and other technology on the devices you use to access the Site and System. This also includes information about your use of the Services, including the type of browser you use, access times, pages viewed, your IP address, and the page you visited before navigating to our Services.
- **Device Data** includes information about the computer or mobile device you use to access our Services, including the hardware model, operating system and version, unique device identifiers, and mobile network information.

The legal bases for collecting and processing of personal data indicated above are: your consent, contract performance with you and our compliance with legal obligations according to Regulation (EU) 2015/847 and Money Laundering and Terrorist Financing Prevention legislation, Company legitimate interests to identify your personalised use of services and devices in order to provide services securely?

WHEN YOU CONTACT US

We collect personal data from or about you when you communicate with us by using the “Contact Us” form on our website, request technical or customer support or otherwise communicate with us. The categories of personal data collected may include your name and email address, as well as any other relevant information contained in the body of your communication.

The lawful legal bases for collecting and processing of the above personal data are: your consent, contract performance with you, or in order to undertake necessary pre-contractual activities.

WHEN YOU SIGN UP FOR UPDATES

For this purpose we may process your name, surname and e-mail address.

The processing of personal data collected as a result of your subscription to our newsletter is based on your consent, which you can withdraw at any time by clicking the “unsubscribe” link at the bottom of the email.

WHEN YOU VISIT OUR WEBSITE

Information collected by cookies and other similar technologies – we use various technologies to collect information which may include saving cookies to users’ computers.

First party cookies – collected by Company website.

The purpose of collecting first party cookies is to remember information about you, such as your language preference or login information.

The legal basis for collecting and processing of the above personal data is based on your consent and our legitimate interest to ensure network and information security.

Third party cookies - collected by Company website.

THIRD PARTIES OR PUBLICLY AVAILABLE SOURCES

We may also obtain information from other sources and combine that with information we collect through our Services. For example, we may collect information about you from third parties, including but not limited to social media platforms and publicly available sources.

We may also receive personal data about you from various third parties and public sources: Identity, Contact, AML / KYC Data from publicly available sources such as public court documents, the public registers of companies, and from electronic data searches, online KYC search tools (which may be subscription or license based), anti-fraud databases and other third party databases, sanctions lists, outsourced third-party KYC service providers and from general searches carried out via online search engines (e.g. Google).

ESTABLISHING AND EVALUATION OF CUSTOMER PROFILES

We are required by the Anti Money Laundering and Counter Terrorism Financing regulations of the UK and EU to take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which our company may be subject and take an informed decision on whether we want to enter into a customer relationship with you, and, if positive, to conduct initial and ongoing screening and monitoring.

During such risk assessment, we must consider various factors relating to a customer and relevant transactions, including the Customer’s location and behavior, his or her being/connection to Politically Exposed or Special Interest Persons, certain types of transactions, etc.

If a significant risk is identified, we may take such measures as freeze the Company Account, stop the transaction, terminate our contract with the customer, or inform the UK Financial Intelligence Unit.

The legal bases for collecting and processing of personal data indicated above are our compliance with legal obligations according to Money Laundering and Terrorist Financing Prevention legislation and Company legitimate interest to prevent use of Company Services for unlawful purposes.

POSSIBLE RECIPIENTS OF YOUR PERSONAL DATA

We shall take appropriate measures to process your personal data in accordance with the applicable law and to ensure that your personal data is not accessed by third parties who do not have the appropriate legal basis for the processing of your personal data.

We do not rent or sell your personal data to anyone.

We may transfer your personal data to the following recipients if this is not in conflict with the applicable laws and regulations:

- our employees and authorised persons processing the personal data specified in this policy within the scope of their competence;
- persons related to the provision of our services and business development (personal data processors or third persons):

Your personal data will be transmitted to third parties that we use to provide our Services; these parties have been rigorously assessed and offer a guarantee of compliance with the legislation on the processing of personal data. These parties have been designated as data processors and carry out their activities according to the instructions given by us and under our control.

The third parties in question belong to the following categories: banking and payment operators, internet providers, companies specialising in IT and SMS services; companies that carry out KYC/AML database checks and fraud database checks;

- We may also be required to share your personal data with various financial institutions and/or law enforcement bodies and officials, supervisory authorities to comply with Anti-Money Laundering, Terrorist Financing and Transfer of Funds laws, prevent fraud or enforce an agreement we have with you;
- We may also share your personal data to comply with applicable laws and regulations, to respond to a legal requests of law enforcement bodies and officials, supervisory authorities, or to other third parties if it is provided by applicable law, and/or if it is relevant for the protection of our and our employees legitimate interests, property or safety, or legitimate interests of third parties or data subject.

Additionally, we may reveal your personal data to third-parties:

- if you request or authorize it;
- to address disputes, claims, or to persons demonstrating legal authority to act on your behalf.

Please note that your information will/will not be transferred outside of the European Union (EU) or the European Economic Area (EEA).

PERSONAL DATA STORAGE AND RETENTION

Your personal data is stored for as long as their storage is required for appropriate purposes for the processing of personal data, as well as in accordance with the applicable law.

When assessing the period of storage of personal data, we take into account existing regulatory requirements, aspects of contractual performance, your instructions (e.g. in the case of consent), and our legitimate interests. If your personal data is no longer needed for the purposes specified, we will delete them or destroy them.

Below, we indicate the most common time limits for the storage of personal data:

- Personal data required for the performance of the contractual obligations: we will keep the Agreement in place until the other storage deadlines are met (see below);
- Records relating to Customer Due Diligence measures and financial transaction records required by Anti Money Laundering and Counter Terrorism Financing regulations of the UK and EU, we keep such information for a minimum of **three year** from the date of the termination of your relationship with us (which would typically arise from the closure/de-registration of your Account on the System), but **no longer than five years**.
- The record of your login information we will keep for periods of **three years** after Company Account will be closed.
- The records related to the transactions retained by Company for periods of **six month** after bank card expiry date.
- A record of your correspondence we will keep for **three months** from the mail date;

YOUR RIGHTS AS DATA SUBJECT REGARDING YOUR PERSONAL DATA

GDPR and other countries' privacy laws provide certain rights for data subjects.

Restoring your personal data

If there are changes to personal data that you have provided to us, please contact us at support@neuronex.io and provide us with the relevant data so that we can achieve the relevant personal data processing purposes.

Your right to access and correct your personal data

In accordance with the provisions of the GDPR, you have the right to require us to have access to your personal data at our disposal, to request their rectification, erasure, processing limitation, to object to the processing of your data, as well as the right to data portability in the cases and procedures set out in the GDPR.

We respect your right to access and control your personal data, so if we receive your request, we will respond to it within the time limits laid down in the regulatory framework (usually not later than one month if there is no specific request that takes longer to prepare the answer), and if it is possible, we will correct or delete your personal data accordingly, or undertake the necessary measures to enable your personal data portability as possible.

You may obtain information about your personal data or exercise other rights as a data subject in one of the following ways:

- by submitting an appropriate application in person and identifying yourself at our office at the address: Harju maakond, Tallinn, Nõmme linnaosa, Kalda tn 9a, 11625, Estonia, each working day from 10-16;
- by submitting an appropriate application to us by post to the following address: Harju maakond, Tallinn, Nõmme linnaosa, Kalda tn 9a, 11625, Estonia;
- by submitting an appropriate application to us by e-mail: support@neuronex.io; it is recommended that you sign it with a secure electronic signature when submitting a relevant application, sending it via e-mail.

Upon receipt of your submission, we will evaluate the content and the possibility of identifying you, and, depending on the situation, we reserve the possibility of asking you to further identify yourself in order to ensure the security and disclosure of your data to the person concerned.

Withdrawal of consent

If the processing of your personal data is based on your consent, you have the right to withdraw it at any time and we will no longer process your personal data processed on the basis of your consent. However, we are informed that the withdrawal of consent cannot affect the processing of personal data which is necessary for the fulfilment of the requirements of regulatory enactments or which is based on a contract, our legitimate interests or other legal bases for the lawful processing of data provided for in regulatory enactments.

COMPLAINTS REGARDING YOUR PERSONAL DATA PROCESSING

If you have any questions or concerns regarding our processing of your personal data, we encourage you to contact us first.

If, however, you believe that we have not been able to resolve the issue with each other and you believe that we are nevertheless in violation of your right to the protection of Personal Data, you have the right a right to lodge a complaint with the appropriate data protection authority.

SAFETY OF YOUR INFORMATION

To help protect the privacy of personal data you transmit through the use of our Site, we maintain physical, technical and administrative safeguards. We update and test our security technology on an ongoing basis. We restrict access to your personal data to those employees who need to know that information to provide services to you. In addition, we train our employees about the importance of confidentiality and maintaining the privacy and security of your data. We commit to taking appropriate disciplinary measures to enforce our employees' privacy responsibilities.

THIRD-PARTY LINKS

Our Site may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy notices, statements or policies.

CHANGES AND UPDATES TO THE PRIVACY POLICY

As our organization and Services may change from time to time, this Privacy policy may be changed as well. We reserve the right to amend it at any time, for any reason, without notice to you, other than the posting of the amended Privacy policy on this Site. We may email periodic reminders of our notices and Terms & Conditions and will email Customers of material changes thereto, but you should check our Site frequently to see the current Privacy policy that is in effect and any changes that may have been made to it.

By using Company's Site and Services, you accept and with this Privacy policy. If you do not agree with this Privacy policy, you should not use this Site or any Company Services.