I. Aim of the Data Protection Policy

As part of its social responsibility, the OÜ NEURONEX PLATFORM, Harju maakond, Tallinn, Nõmme linnaosa, Kalda tn 9a, 11625, Estonia committed to international compliance with data protection laws. This Data Protection Policy applies worldwide to the OÜ NEURONEX PLATFORM and is based on globally accepted, basic principles on data protection. Ensuring data protection is the foundation of trustworthy business relationships and the reputation of the OÜ NEURONEX PLATFORM.

The Data Protection Policy provides one of the necessary framework conditions for cross-border data transmission among the Group companies. It ensures the adequate level of data protection prescribed by the European Union Data Protection Directive, EU's General Data Protection Regulation (GDPR) and the national laws for cross-border data transmission, including in countries that do not yet have adequate data protection laws.

II. Scope and amendment of the Data Protection Policy

This Data Protection Policy applies to all companies of the OÜ NEURONEX PLATFORM, all of its dependent Group companies, affiliated companies and their employees. "Dependent" in this instance means that OÜ NEURONEX PLATFORM may enforce the adoption of this Data Protection Policy directly or indirectly, on the basis of voting majority, majority management representation, or by agreement. The Data Protection Policy extends to all processing of personal data.

In countries where the data of legal entities is protected to the same extent as personal data, this Data Protection Policy applies equally to data of legal entities. Anonymized data, e.g. for statistical evaluations or studies, is not subject to this Data Protection Policy. Individual Group companies are not entitled to adopt regulations that deviate from this Data Protection Policy. Additional data protection policies can be created in agreement with the Chief Officer Corporate Data Protection only if required by applicable national laws. This Data Protection Policy can be amended under the defined procedure for amending policies. The amendments will be reported immediately to the OÜ NEURONEX PLATFORM companies using the process for amending policies. Amendments that have a major impact on compliance with the Data Protection Policy must be reported annually to the data protection authorities that issue approval for this Data Protection Policy as Binding Corporate Rules. The latest version of the Data Protection Policy can be accessed with the data privacy information at OÜ NEURONEX PLATFORM's website: www.neuronplatform.com

III. Application of national laws

This Data Protection Policy comprises the internationally accepted data privacy principles without replacing the existing national laws. It supplements the national data privacy laws. The relevant national law will take precedence in the event that it conflicts with this Data Protection Policy, or it has stricter requirements than this Policy. The content of this Data Protection Policy must also be observed in the absence of corresponding national legislation. The reporting requirements for data processing under national laws must be observed. Each company of OÜ NEURONEX PLATFORM is responsible for compliance with this Data

Protection Policy and the legal obligations. If there is reason to believe that legal obligations contradict the duties under this Data Protection Policy, the relevant Group company must inform appropriate personnel. In the event of conflicts between national legislation and the Data Protection Policy, OÜ NEURONEX PLATFORM will work with the relevant Group company to find a practical solution that meets the purpose of the Data Protection Policy.

IV. Principles for processing personal data

1. Fairness and lawfulness

When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.

2. Restriction to a specific purpose

Personal data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.

3. Transparency

The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of, or informed of:

» The identity of the Data Controller
» The purpose of data processing
» Third parties or categories of third parties to whom the data might be transmitted

4. Data reduction and data economy

Before processing personal data, you must determine whether and to what extent the processing of personal data is necessary in order to achieve the purpose for which it is undertaken.

Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data must be used. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by national law.

5. Deletion

Personal data that is no longer needed after the expiration of legal or business process-related periods must be deleted. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.

6. Factual accuracy; up-to-dateness of data

Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

7. Confidentiality and data security

Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

V. Reliability of data processing

Collecting, processing and using personal data is permitted only under the following legal bases. One of these legal bases is also required if the purpose of collecting, processing and using the personal data is to be changed from the original purpose.

1. Customer and partner data

1.1 Data processing for a contractual relationship

Personal data of the relevant prospects, customers and partners can be processed in order to establish, execute and terminate a contract. This also includes advisory services for the partner under the contract if this is related to the contractual purpose. Prior to a contract – during the contract initiation phase – personal data can be processed to prepare bids or purchase orders or to fulfill other requests of the prospect that relate to contract conclusion. Prospects can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by the prospects must be complied with. For advertising measures beyond that, you must observe the following requirements under V.1.2.

1.2 Data processing for advertising purposes

If the data subject contacts a OÜ NEURONEX PLATFORM company to request information (e.g. request to receive information material about a product), data processing to meet this request is permitted. Customer loyalty or advertising measures are subject to further legal requirements. Personal data can be processed for advertising purposes or market and opinion research, provided that this is consistent with the purpose for which the data was originally collected. The data subject must be informed about the use of his/her data for advertising purposes. If data is collected only for advertising purposes, the disclosure from the data subject is voluntary. The data subject shall be informed that providing data for this purpose is voluntary. When communicating with the data subject, consent shall be obtained from him/her to process the data for advertising purposes. When giving consent, the data subject should be given a choice among available forms of contact such as regular mail, e-mail and phone (Consent, see V.1.3). If the data subject refuses the use of his/her data for advertising purposes, it can no longer be used for these purposes and must be blocked from use for these purposes. Any other restrictions from specific countries regarding the use of data for advertising purposes must be observed.

1.3 Consent to data processing

Data can be processed following consent by the data subject. Before giving consent, the data subject must be informed in accordance with this Data Protection Policy. The declaration of consent must be obtained in writing or electronically for the purposes of documentation.

In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

1.4 Data processing pursuant to legal authorization

The processing of personal data is also permitted if national legislation requests, requires or allows this. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions.

VI. Transmission of personal data

Transmission of personal data to recipients outside or inside the OÜ NEURONEX PLATFORM is subject to the authorization requirements for processing personal data. The data recipient must be required to use the data only for the defined purposes. In the event that data is transmitted to a recipient outside the OÜ NEURONEX PLATFORM to a third country this country must agree to maintain a data protection level equivalent to this Data Protection Policy. This does not apply if transmission is based on a legal obligation. A legal obligation of this kind can be based on the laws of the domiciliary country of the Group company transmitting the data. In the alternative, the laws of the domiciliary country of the Group company can acknowledge the purpose of data transmission based on the legal obligation of a third country. If data is transmitted by a third party to a OÜ NEURONEX PLATFORM company, it must be ensured that the data can be used for the intended purpose. If personal data is transferred from a Group company with its registered office in the European Union/European Economic Area to a Group company with its registered office outside of the European Economic Area (third country), the company importing the data is obligated to cooperate with any inquiries made by the relevant supervisory authority in the country in which the party exporting the data has its registered office, and to comply with any observations made by the supervisory authority with regard to the processing of the transmitted data. The same applies to data transmission by Group companies from other countries. If they are part of an international certification system for binding corporate rules on data protection, they must ensure cooperation with the relevant auditing offices and agencies.

In the event that a data subject claims that this Data Protection Policy has been breached by the Group company located in a third country that is importing the data, the Group company located in the European Economic Area that is exporting the data undertakes to support the party concerned, whose data was collected in the European Economic Area, in establishing the facts of the matter and also asserting his/her rights in accordance with this Policy against the Group company importing the data. In addition, the data subject is also entitled to assert his or her rights against the Group company exporting the data. In the event of claims of a violation, the company exporting the data must document to the data subject that the company importing the data in a third country (in the event that the data is further processed after receipt) did not violate this Data Protection Policy. In the case of personal data being transmitted from a Group company located in the European Economic Area to a Group

company located in a third country, the data controller transmitting the data shall be held liable for any violations of this Policy committed by the Group company located in a third country with regard to the data subject whose data was collected in the European Economic Area, as if the violation had been committed by the data controller transmitting the data. The legal venue is the responsible court where the company exporting the data is located.

VII. Contract data processing

Data processing on Behalf means that a provider is hired to process personal data, without being assigned responsibility for the related business process. In these cases, an agreement on Data Processing on Behalf must be concluded with external providers and among companies within the OÜ NEURONEX PLATFORM. The client retains full responsibility for correct performance of data processing. The provider can process personal data only as per the instructions from the client. When issuing the order, the following requirements must be complied with; the department placing the order must ensure that they are met.

1. The provider must be chosen based on its ability to cover the required technical and organizational protective measures.
2. The order must be placed in writing. The instructions on data processing and the responsibilities of the client and provider must be documented.
3. The contractual standards for data protection provided by the Chief Officer Corporate Data Protection must be considered.
4. Before data processing begins, the client must be confident that the provider will comply with the duties. A provider can document its compliance with data security requirements in particular by presenting suitable certification. Depending on the risk of data processing, the reviews must be repeated on a regular basis during the term of the contract.
5. In the event of cross-border contract data processing, the relevant national requirements for disclosing personal data abroad must be met. In particular, personal data from the European Economic Area can be processed in a third country only if the provider can prove that it has a data protection standard equivalent to this Data Protection Policy. Suitable tools can be: a. Agreement on EU standard contract clauses for contract data processing in third countries with the provider and any subcontractors.

b. Participation of the provider in a certification system accredited by the EU for the provision of a sufficient data protection level.

c. Acknowledgment of binding corporate rules of the provider to create a suitable level of data protection by the responsible supervisory authorities for data protection.

VIII. Rights of the data subject

Every data subject has the following rights. Their assertion is to be handled immediately by the responsible unit and cannot pose any disadvantage to the data subject.

1. The data subject may request information on which personal data relating to him/her has been stored, how the data was collected, and for what purpose. If there are further rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws, these will remain unaffected.

2. If personal data is transmitted to third parties, information must be given about the identity of the recipient or the categories of recipients.
3. If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.
4. The data subject can object to the processing of his or her data for purposes of advertising or market/opinion research. The data must be blocked from these types of use.
5. The data subject may request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.
6. The data subject generally has a right to object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

Additionally, every data subject can assert the rights as a third-party beneficiary if a company that has agreed to comply with the Data Protection Policy does not observe the requirements and violates the party's rights.

XII. Data protection incidents

All employees must inform their supervisor, data protection coordinator immediately about cases of violations against this Data Protection Policy or other regulations on the protection of personal data (data protection incidents).

The manager responsible for the function or the unit is required to inform the responsible data protection coordinator or the Chief Officer Corporate Data Protection immediately about data protection incidents.

In cases of

» improper transmission of personal data to third parties,
» improper access by third parties to personal data, or
» loss of personal data

the required company reports (Information Security Incident Management) must be made immediately so that any reporting duties under national law can be complied with.

XIII. Responsibilities and sanctions

The executive bodies of the Group companies are responsible for data processing in their area of responsibility. Therefore, they are required to ensure that the legal requirements, and those contained in the Data Protection Policy, for data protection are met (e.g. national reporting duties). Management staff are responsible for ensuring that organizational, HR, and technical measures are in place so that any data processing is carried out in accordance with data protection. Compliance with these requirements is the responsibility of the relevant employees.

The relevant executive bodies must inform as to the name of their data protection coordinator . Organizationally speaking, this task can be performed by a data protection

coordinator for multiple companies or plants. The data protection coordinators are the contact persons on site for data protection. They can perform checks and must familiarize the employees with the content of the data protection policies.
The departments responsible for business processes and projects must inform the data protection coordinators in good time about new processing of personal data. For data processing plans that may pose special risks to the individual rights of the data subjects, the Chief Officer Corporate Data Protection must be informed before processing begins. This applies in particular to extremely sensitive personal data. The managers must ensure that their employees are sufficiently trained in data protection. Improper processing of personal data, or other violations of the data protection laws, can be criminally prosecuted in many countries and result in claims for compensation of damage. Violations for which individual employees are responsible can lead to sanctions under employment law.

XIV. Definitions

» Data is anonymized if personal identity can never be traced by anyone, or if the personal identity could be recreated only with an unreasonable amount of time, expense and labor.
» Consent is the voluntary, legally binding agreement to data processing.
» Data protection incidents are all events where there is justified suspicion that personal data is being illegally captured, collected, modified, copied, transmitted or used. This can pertain to actions by third parties or employees.
» Data subject under this Data Protection Policy is any natural person whose data can be processed. In some countries, legal entities can be data subjects as well.
» The European Economic Area (EEA) is an economic region associated with the EU, and includes
Norway, Iceland and Liechtenstein.
» Highly sensitive data is data about racial and ethnic origin, political opinions, religious or philosophical beliefs, union membership or the health and sexual life of the data subject. Under national law, further data categories can be considered highly sensitive or the content of the data categories can be structured differently. Moreover, data that relates to a crime can often be processed only under special requirements under national law.
» Personal data is all information about certain or definable natural persons. A person is definable for instance if the personal relationship can be determined using a combination of information with even incidental additional knowledge.
» Processing personal data means any process, with or without the use of automated systems, to collect, store, organize, retain, modify, query, use, forward, transmit, disseminate or combine
and compare data. This also includes disposing of, deleting and blocking data and data storage media.
» Processing personal data is required if the permitted purpose or justified interest could not be achieved without the personal data, or only with exceptionally high expense.
» Data Controller is the legally independent company of the OÜ NEURONEX PLATFORM, whose business activity initiates the relevant processing measure.

» A sufficient level of data protection in third countries is acknowledged by the EU Commission if the core of personal privacy, as unanimously defined in the member countries of the EU is adequately ensured. When making its decision, the EU Commission accounts for all circumstances that play a role in data transmission or a category of data transmission. This includes the opinions under national law and relevant applicable professional standards and security measures.
» Third countries under the Data Protection Policy are all nations outside the European Union/ EEA. This does not include countries with a data protection level that is considered sufficient by the EU Commission.
» Third parties are anyone apart from the data subject and the Data Controller. In a case of Data Processing in Behalf data processors in the EU are not third parties under the data protection laws, because they are assigned by law to the responsible entity.
» Transmission is all disclosure of protected data by the responsible entity to third parties.