Personal Data Processing Policy of Netera Systems s.r.o.

In accordance with Act. No. 110/2019 Sb., on Personal Data Processing, as amended, in connection with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Processing Regulation) - hereinafter referred to as "GDPR"

The purpose of this Personal Data Processing Policy (hereinafter referred to as the "**Policy**") is to provide (potential) clients, visitors to the website www.neterapay.eu and business partners with information explaining how **Netera Systems s.r.o.**, company ID no. 242 26,726, registered in the Commercial Register maintained with the Municipal Court in Prague, section C, insert 238789, with registered office at: Sudoměřská 1293/32, Žižkov, 130 00 Praha 3 (hereinafter referred to as "Controller"), processes personal data.

Contact details of the Controller:

e-mail: podpora@neterapay.eu

The Controller has appointed a data protection officer, Jan Rožumberský.

Contact details of the Data Protection Officer:
gdpr@neterapay.eu

Whose personal data does the Controller process?
The Controller processes personal data in particular of the following data subjects (hereinafter referred to as the "**Data Subject**"):
- website visitor,
- Client,
- a person who has given their consent to the processing of personal data,
- a business partner.

To what extent does the Controller process personal data?

The Controller processes only such personal data for the processing of which it has the legal title in accordance with applicable legislation. It processes personal data fairly and transparently, only for the intended purpose, securely and only for as long as required by the law or as specified in this Policy.

As regards the website visitor, the Controller processes in particular:
- IP address, cookies

As regards the Client, the Controller primarily processes personal data that have been disclosed thereto (or its processor) by the Client or in any form or ascertained about the Client by third parties, identically in connection with the provision of the Controller's services. The Controller is also entitled to process personal data necessary for the provision of its services to the extent of data obtained by the Controller (or its processor) from publicly available sources. This includes in particular the following personal data:

- name, surname, date of birth, place of birth, birth certificate number, permanent address, nationality, gender,
- telephone number, e-mail address, contact address (if different from the address of permanent residence), address for delivery of the activation code,
- details of the identity card on the basis of which the identity of the Data Subject can be verified: card number, validity of the card, issuer (authority), copy of the card,
- details of the additional identity document (depending on the type of document): type of document, validity, number of the document if applicable, issuer of the document if applicable, copy of the document
- data on the political exposure of the Data Subject and other specific information required by applicable legal regulations,
- NeteraPay wallet number,
- bank account numbers (for a bank account, the Controller may also require a copy of proof of the existence of the account),
- records of communications with the Data Subject,
- IP address, cookies.

Within the application of the "Know your client" principle pursuant to Act No. 253/2008 Sb., on Certain Measures against Money Laundering and Terrorist Financing, as amended (hereinafter referred to as the "AML Act"), the Controller may request data on:
- the purpose for which the account was established,
- the origin of the funds,

- where applicable, the field of activity.

For the purpose of fulfilling other obligations under the AML Act, the Controller is also entitled to request data on:
- the annual amount of net income,
- the predominant origin of the funds to be deposited into the electronic wallet,
- where applicable, data on the sale of property, inheritance or other source of funds, i.e. the frequency of income and its amount.

As regards the person who has given their consent to the processing of personal data, the Controller shall only process personal data for processing of which the person has given their consent, unless the Controller has a legal title for processing personal data other than the consent.

For what purpose the Controller processes personal data

The purpose of the processing of personal data by the Controller is in particular:
- identification of the Data Subject,
- verification of the Data Subject's personal data,
- assessing the (potential) Client's request for the provision of services by the Controller,
- profiling of the Data Subject,
- use of personal data for the purpose of profiling a subsequent business offer,
- fulfilment of mutual contractual relationship between the Client and the Controller,
- fulfilment of contractual relationship between the Controller and a third party,
- fulfilment of statutory obligations of the Controller or third parties,
- fraud prevention,
- customer support,
- protecting the legitimate interests of the Controller or third parties,
- asserting legal claims and obligations under the contractual relationship between the Controller and the Client.

On the basis of which legal title does the Controller process personal data?

The legal basis for the processing of personal data is based on Article 6 of the GDPR, in particular
- Article 6(1)(a) GDPR, where the Data Subject has given consent to the processing of their personal data for one or more specific purposes,
- Article 6(1)(b) GDPR, the processing is necessary for the performance of contracts to which the Data Subject as Client is a contracting party or for the implementation of measures taken prior to the conclusion of the contract at the request of the Data Subject as Client,
- Article 6(1)(c) of the GDPR, the processing is necessary for compliance with legal obligations to which the Controller is subject, in particular obligations arising under the AML Act,
- Article 6(1)(f) of the GDPR, the processing is necessary for the purposes of the legitimate interests of the Controller or a third party, unless those interests are overridden by the interests and fundamental rights and freedoms of the Data Subject requiring the protection of personal data (for example, the processing of photographs and copies of identity cards, records of communications or processing for marketing purposes).

If the processing of personal data on the basis of legitimate interest involves so-called profiling within the meaning of Article 22 of the GDPR, the Data Subject has the right to object to such processing at any time. In the event of asserting an objection, the Controller shall no longer process the data unless it demonstrates compelling legitimate grounds for the processing which override the interests or rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims, but this shall not apply in the case of direct marketing. If the processing for direct marketing or profiling purposes is objected to by the Data Subject, personal data will no longer be processed for these purposes.

Personal data are processed systematically and automatically by the Data Controller. In particular, when processing for direct marketing purposes and when executing the risk assessment of the Client (Data Subject) according to the AML Act, so-called profiling within the meaning of Article 22 of the GDPR may also happen.

In connection with direct marketing, the Data Subject has the right to refuse further marketing and commercial communications from the Controller at any time.

Does the Controller process copies of identity documents?

Pursuant to Act No. 269/2021 Sb, on identity cards, as amended, and Act No. 329/1999 Sb., on travel documents, as amended, the Controller is entitled to make and further process a copy of an identity card/travel document, or other identity document, and the data contained in the copy only if the Data Subject gives their explicit consent to do so, unless a special legal regulation provides otherwise. The Data Subject is entitled to withdraw their consent at any time without giving any reason.

The Data Subject's consent pursuant to the preceding paragraph is not required if the Controller processes a copy or extracts from the submitted (identity) documents for the purposes of the AML Act (Section 8(11) of the AML Act).

If the Data Subject gives consent to the Controller to process a copy of the identity documents, the Data Subject consents to the use (even repeatedly) of the copies of the identity documents and other documents within the meaning of the preceding paragraph (including the personal data contained therein), in particular for the purpose of verifying their identity and for the purpose of preventing crime. The use of the copy of the identity document is therefore necessary for the performance of contracts to which the Client is or will be a party, for the fulfilment of legal obligations to which the Controller is subject, in particular the obligations arising under the AML Act and Act No. 370/2017 Sb., on Payment System, as amended, or to protect the Client's important interests and the Controller's rights.

For how long are personal data processed by the Controller?

Personal data are processed by the Controller for different periods of time depending on their purpose. Unless the length of processing is determined by the consent given by the Data Subject, the Controller processes personal data only for the time necessary to fulfil the purpose of processing, i.e. in particular for the duration of the contractual relationship between the Client and the Controller or for the period of compliance with legal obligations. In addition, for the period of time specified by the applicable legal regulations.

Unless otherwise specified, personal data shall be deleted by the Controller no later than within one month after the purpose or legal reason for their processing ceases to exist.

Personal data that are subject to archiving obligations are processed for the period specified by the applicable legal regulations.

The statutory period for the retention of data and documents for the purpose of identification and fulfilment of other obligations set out in the AML Act is 10 years following the end of the calendar year in which the contractual relationship between the Client and the Controller was terminated.

Personal data for the retention of which the consent of the Data Subject is necessary shall be retained for the period of validity of the consent to their retention. This shall not mean, however, that after withdrawal of consent the Controller is not entitled to process or retain personal data for any other reason. If the consent to the processing of personal data is withdrawn and there is no other reason for processing the personal data, the personal data concerned shall be deleted no later than in one month of receiving the withdrawal of the consent by the Controller.

To whom does the Controller transfer personal data?

On the basis of consent, in connection with the performance of obligations set out in the applicable legal regulations or if the legitimate interest of the Controller or a third party so requires, the Controller is entitled to transfer personal data to third parties.

The recipients of personal data include in particular:
- IT service providers,
- providers of filing and archiving services,
- providers of significant activities (outsourcing),
- lawyers, notaries, bailiffs,
- public authorities,
- providers of printing and mailing services, including couriers,
- contractual business partners of the Controller.

More detailed and up-to-date specification of processors and other recipients will be provided by the Controller to the Data Subject upon request.

The Controller wishes to point out that it is not responsible for the processing of personal data by third parties who are in the position of the Data Controller. Such processing of personal data will be subject to the third party's own personal data protection policy in its capacity as controller.

Personal data will not be transferred to third countries outside the EU.

What rights does the Data Subject have?

The Data Subject has the right to:

a. request access to the personal data processed by the Controller,

b. request a copy of the personal data from the Controller,

c. request the Controller for confirmation of the personal data processed, in particular to communicate the purpose of the processing, the category of personal data concerned, the recipient or category of recipients, the period of processing/retention of the personal data, information on the source of the personal data, whether automated decision-making, including profiling, is taking place,

d. request the Controller to rectify or complete any inaccuracies,

e. request the Controller to erase the personal data processed by the Controller if they are no longer necessary for the purpose provided or if they are processed unlawfully by the Controller,

f. request the Controller to restrict the processing of their personal data in the cases provided for in Article 18 of the GDPR,

g. the portability of their personal data,

h. object pursuant to Article 21 of the GDPR.

If the Data Subject believes that the Controller is processing personal data in violation of their rights or the law, the Data Subject may:

a. request an explanation from the Controller,

b. request that the unlawful situation be rectified,

c. lodge a complaint with the supervisory authority, which is the Office for Personal Data Protection.

The Data Subject has the right to withdraw their consent to the processing of personal data at any time. However, any withdrawal of consent shall not affect the lawfulness of the processing of personal data prior to such withdrawal of consent. Any withdrawal of consent shall also not affect the lawfulness of the processing of personal data for any other legal ground.

The Data Subject may withdraw their consent to the processing of personal data in paper or electronic form by submitting it to one of the contact details listed in this Policy. The Data Subject acknowledges that if the Controller is in doubt as to whether the consent has been withdrawn by the person entitled to do so, the Controller is entitled to verify the identity of the sender by any other appropriate means. This also applies in relation to the form and manner of exercising other rights under this Policy.

The Data Subject acknowledges that the Controller has 30 days from the receipt of the request(s) to process the request(s).

This Policy shall apply as of 1 April 2022 until revoked and supersede all previous Policies.

Date of last update: 14 January 2022.