

NEOPAY PRIVACY POLICY

Effective as of 22 October 2025.

This Privacy Policy (hereinafter referred to as the Policy) defines how NEO Finance, AB (hereinafter referred to as NEO Finance, the Company, we) processes the personal data of its customers and other persons who are interested in the Company, its services or use payment initiation and account information or other open banking services provided by Neopay, i.e., personal data of payment service recipients, business partners, representatives of service providers, as well as persons who visit our website <https://neopay.online> (hereinafter referred to as the Website). The Policy stipulates the principles, rules and requirements for the processing of personal data that the Company adheres to in order to ensure the security of your personal data and the protection of your rights when using the Neopay payment initiation and account information services (hereinafter referred to as the Services).

Data Controller

NEO Finance, AB (legal entity code 303225546, Ukmergės St. 126, LT-08100, Vilnius, e-mail: info@neopay.online) is the controller of your personal data.

If you have any questions about the processing of your personal data or exercising your rights, please contact our data protection officer by e-mail: asmensduomenys@neofinance.lt.

WHO ARE WE?

NEO Finance is an electronic money institution (Electronic Money Institution License No. 7, issued on 5 January 2017) which provides payment initiation, account information and other open banking services regulated by the Rules for the Provision of Open Banking Services using Neopay trademark (<https://www.neopay.online/lt/legal/terms-of-service>).

We do care about your privacy and the security of your personal data, and we are fully committed to processing the personal data of our customers and other persons (potential customers, persons interested in our services) in accordance with the established principles and requirements for the processing of personal data, and we ensure the confidentiality of personal data by implementing appropriate technical and organisational measures to protect personal data from unauthorised access, disclosure, accidental loss, alteration or destruction, or other unlawful processing. Please take the time to carefully read this Policy and familiarize yourself with the terms and conditions of your personal data processing.

Additional information may be provided in payment service agreements and other contracts, cookie policies, personal data processing consents or separate privacy notices. This Privacy Policy applies in combination with our other documents.

WHAT PRINCIPLES DO WE FOLLOW WHEN PROCESSING PERSONAL DATA?

We respect your privacy and only collect and process personal data that is necessary to achieve the specified data processing purposes. When processing your personal data, we comply with applicable laws and regulations, including the General Data Protection Regulation (hereinafter referred to as the GDPR, Regulation), the Law on Legal Protection of Personal Data of the Republic of Lithuania, and other legal acts regulating the security of personal data. When processing Personal Data, we adhere to the principles of personal data processing set out in the Regulation:

- We process your Personal Data in a lawful, fair and transparent manner;
- We collect your Personal Data for specified, explicit and legitimate purposes and do not process it in a manner that is incompatible with those purposes, except to the extent permitted by legal acts;
- We ensure that Personal Data is adequate, relevant and is only necessary for the purposes of the processing we have specified, i.e. we do not collect or store excessive or unnecessary data;
- We take all necessary measures to correct or delete Personal Data that is inaccurate or incorrect;
- We store data only for as long as is necessary to achieve the specified purposes;
- We apply the necessary technical and organisational security measures to ensure the security of your Personal Data, including protection against unauthorised or unlawful data processing and against accidental loss, destruction or damage, including granting access to data or transferring data only to those employees or service providers who need such access due to their job functions or services provided.

WHEN DO WE PROCESS YOUR PERSONAL DATA?

We collect and process your personal data only when it is necessary to achieve the specified legitimate purposes and when we have a legal basis for doing so. The Company may process personal data when:

- it is necessary to perform an agreement concluded with you or to take action at your request prior to concluding an agreement;
- we are required to do so by legal acts;
- it is necessary to process personal data for the legitimate interests of the Company or third parties;
- you have given your consent to the processing of personal data for the specified purpose or purposes.

Personal data may be obtained directly from you, for example, when you use our services, enter into agreements with us on your own behalf or on behalf of others, send us your curriculum vitae (CV) or other information related to employment, or otherwise contact us with inquiries, communicate with us via social networks, or simply follow our activities on social networks, or visit the Company.

We may also obtain your personal data indirectly, for example, from persons you represent; your spouses; data processors; persons working under an individual activity certificate or self-employment certificate who submit financial documents to the Company for the assessment of their solvency; when you receive payments where the Company acts as a payment service provider, etc. We may also obtain your personal data from separate databases, registers and information systems, as well as other external sources, including, but not limited to: the Bank of Lithuania, other financial institutions and lists of international sanctions.

Please note that you are not required to provide any personal data, but this may prevent us from providing you with services and achieving other specified goals.

WHAT PERSONAL DATA DO WE PROCESS?

The scope of personal data processed, including data categories, and the processing operations we perform with personal data (collection, use, storage, sharing, transfer, etc.) depend on who you are, our relationship with you, and the services you use or are interested in, whether you are our customer, or simply visited our website looking for information and (or) contacted us for additional information, or are participating in our announced selection process for a vacant position in the Company.

PROCESSING OF PERSONAL DATA WHEN USING NEOPAY SERVICES

CONCLUSION AND EXECUTION OF AN ELECTRONIC MONEY ACCOUNT AND/OR PAYMENT SERVICE AGREEMENT

When you decide to open an e-money account with us and/or enter into a payment services agreement, depending on whether you are a natural person opening an account and entering into an agreement on your own behalf, or a legal entity wishing to open a corporate account, we process

If you are a natural person	If you are a legal person
• Name, surname • Personal number / Date of birth; • E-mail address • Telephone number • Place of residence • Nationality • Personal identification document number (ID card or passport) • Individual activity certificate number • Electronic money account number (opening date, money turnover) • Account transaction limits • Current account number at another credit institution • Password	• Contact person (name, surname, position, telephone number, e-mail address) • Details of the signatory (name, surname, telephone number, nationality, personal number (if not applicable – date of birth), signature) • Details of the head of the legal entity (name, surname, personal number/date of birth, telephone number, e-mail address, address, nationality, copy of personal identification document) • Details of the final beneficiary (name, surname, personal number/date of birth, e-mail address, address, nationality, copy of personal identification document)

- Signature

Purpose of data processing	To conclude and execute an agreement for the provision of electronic money and payment services
Legal basis for data processing	Article 6(1)(b) of the GDPR – processing is necessary for the performance of a contract or in order to take steps at the request of the data subject prior to entering into a contract
Data retention period	10 years after termination of the agreement and end of business relations/closure of the account

IDENTIFICATION, PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING, IMPLEMENTATION OF THE “KNOW YOUR CUSTOMER” PRINCIPLE

As a financial institution, we are required to verify each potential customer in accordance with the requirements of the money laundering and terrorist financing prevention and related legal acts (hereinafter referred to as MLTFP requirements), including identification of the potential customer.

When providing our services, we are required to collect specific personal data and information and to perform mandatory procedures established by MLTFP requirements – customer identification, implementation of the “Know Your Customer” (KYC) principle, and continuous monitoring of the customer and customer operations (transactions) to ensure that they comply with the risk profile and financial situation of the customer, and the information about the customer available to the Company, allowing us to identify unusual or suspicious transactions. For this purpose, we collect and process the following personal data:

If you are a natural person	If you are a legal person
• Name, surname, personal number, date of birth, nationality, address, copy of personal identification document, personal identification document details, customer and beneficiary identification questionnaire details, personal identification features (online, e-signature/mobile signature using Idenfy services), remote identification: e-signature/mobile signature details; image data (image of the person (face) and signature), photo of the personal identification document, time and date of image transmission); bank account payment details, value of transactions executed, whether the person holds public office or whether he/she or a member of his/her family is a politically exposed person (PEP), risk group, anthroponym, alternative names, reason for rejection of identification, date and time of identification, IP address, browser data, publication of a search for the person	• Name and code of the company • Name and surname of the representative of the legal entity, documents confirming representation, data from the customer and beneficiary identification questionnaire, data of the head of the customer (name, surname, personal number/date of birth, nationality, personal identification document data, identification features (online, e-signature/mobile signature, markID), remote identification: e-signature/mobile signature data; image data (image of the person (photo of the face), photo of the personal identity document, time and date of image transmission); bank account payment data), whether he/she holds public office or whether he/she or a member of his/her family is a politically exposed person (PEP) • Name, surname, personal number, date of birth, nationality, address of the beneficiary, data from the customer and beneficiary identification questionnaire, e-signature data, remote identification: e-signature data; image data (image of the person (photo of the face), photo of the personal identity document, time and date of image transmission), sources of funds/income, whether the person holds public office, risk group, anthroponym, alternative names, shares held, a

Purpose of data processing	Customer onboarding – identification, implementation of money laundering and terrorist financing prevention, “Know Your Customer” principle requirements
Legal basis for data processing	Article 6(1)(c) of the GDPR – legal obligation applicable to the Company (Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania, Law on International Sanctions of the Republic of Lithuania)
Data retention period	8 years from the end of transactions or contractual/business relationships with the customer

BY IMPLEMENTING THE “KNOW YOUR CUSTOMER” (KYC) PRINCIPLE ESTABLISHED BY LEGAL ACTS AND THE REQUIREMENTS FOR THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING, WE CONTINUOUSLY MONITOR OUR BUSINESS RELATIONSHIPS AND FINANCIAL TRANSACTIONS OF THE CUSTOMER AND UPDATE THE DATA.

In accordance with the “Know Your Customer” (KYC) principle and MLTFP requirements established by legal acts, we are obliged to continuously monitor business relationships and financial transactions of the customer and to regularly update data. For this purpose, we collect and process the following personal data: data provided in the customer and beneficiary identification questionnaire, anthroponym, alternative names, a part of other rights in a legal entity.

Purpose of data processing	Monitoring of business relationships and financial transactions of the customer and updating of data
Legal basis for data processing	Article 6(1)(c) of the GDPR – legal obligation applicable to the Company (Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania, Law on International Sanctions of the Republic of Lithuania)
Data retention period	8 years from the end of transactions or contractual/business relationships with the customer

PROVISION OF PAYMENT INITIATION SERVICES

For the purposes of payment initiation, authentication of service users (payers), payment initiation services, and provision of services to customers and users (payers), we process the following personal data of payers:

If you are a natural person	If you are a legal person
- name and surname of the payer; account number of the payer, purpose of payment; account management institution selected by the payer; unique financial transaction number, currency, payment date, IP address; - title/name and surname of the recipient, account number.	- name, surname, position, e-mail, telephone number of the representative, currency, payment date, IP address, account number - title/name and surname of the recipient, account number.

Purpose of data processing	Provision of payment initiation services
Legal basis for data processing	Article 6(1)(b) of the GDPR – processing is necessary for the performance of a contract or in order to take steps at the request of the data subject prior to entering into a contract Article 6(1)(c) of the GDPR – legal obligation applicable to the Company (Law on Payment of the Republic of Lithuania)
Data retention period	3 years after the payment transaction

Recipients of personal data: in the case of payment initiation services, your personal data is transferred to the recipients of the transferred funds (i.e., customers of the Company or other third parties whose goods or services you purchase).

PROVISION OF ACCOUNT INFORMATION SERVICES

For the purpose of provision of account information services, authentication of account information service users, servicing of account information service customers and users, we process the following personal data of service users:

If you are a natural person	If you are a legal person
name, surname, personal number, address, date of birth, account management institution, account number, and selected account information, payments made and their history.	name, surname, position, e-mail address, telephone number of the representative

Purpose of data processing	Provision of account information services
Legal basis for data processing	Article 6(1)(b) of the GDPR – processing is necessary for the performance of a contract or in order to take steps at the request of the data subject prior to entering into a contract Article 6(1)(c) of the GDPR – legal obligation applicable to the Company (Law on Payment of the Republic of Lithuania) Article 6(1)(a) of the GDPR – your consent as a data subject (in the case of data transfer to third parties)
Data retention period	3 years

PAYER CARD CONFIRMATION (PCOV SERVICE PROVISION)

For this purpose, we collect and process the following personal data: name, surname, personal number, date of birth, address, account management institution, account number and selected account information, payments made and their history, card number (masked).

Purpose of data processing	Confirmation of a payment card
Legal basis for data processing	Article 6(1)(c) of the GDPR – legal obligation applicable to the Company (Law on Payment of the Republic of Lithuania)
Data retention period	3 years

IDENTIFICATION OF A NEW USER (PROVISION OF 12PLAY SERVICES TO ONLINE GAMBLING SERVICE PROVIDERS)

For this purpose, we collect and process the following personal data: name, surname, personal number, nationality, telephone number

Purpose of data processing	Identification of a new user seeking to use gambling services
Legal basis for data processing	Article 6(1)(a) of the GDPR – consent of the data subject
Data retention period	30 Days

PERSONAL NUMBER VERIFICATION (PCSP SERVICE PROVISION)

For this purpose, we collect and process the following personal data: name, surname, personal number

Purpose of data processing	Confirmation of a personal number
Legal basis for data processing	Article 6(1)(c) of the GDPR – legal obligation applicable to the Company (Law on Payment of the Republic of Lithuania)
Data retention period	10 years

EXAMINATION OF COMPLAINTS

In order to ensure the proper examination and administration of complaints, we process the following personal data of customers of the Company and other persons who have submitted complaints: name, surname, address, telephone number, e-mail address, date of complaint, other personal data provided in the complaint and (or) required to examine the complaint, technical data (if the complaint is submitted electronically - IP address, location, device, browser, etc.).

Purpose of data processing	Examination of a complaint from a customer or other person
Legal basis for data processing	Article 6(1)(c) of the GDPR – Legal obligation applicable to the Company (Resolution No. 03-105 of the Board of the Bank of Lithuania of 6 June 2013) (personal data is processed on this basis when a customer or third party submits a complaint about the services provided by the Company)
Data retention period	3 years after the complaint has been examined

ADMINISTRATION OF THE SELF-SERVICE AREA

In order to ensure the functionality and administration of the Customer self-service area, we process the following personal data of customers (legal entities) of the Company: name, surname, company, position, e-mail address, telephone number, password, self-service login details (date, time, actions performed in the system), IP address.

Purpose of data processing	Proper administration of the Neopay customer self-service area
Legal basis for data processing	Article 6(1)(b) of the GDPR – processing is necessary for the performance of a contract or in order to take steps at the request of the data subject prior to entering into a contract
Data retention period	During the term of the agreement and for 10 years after the expiry of the agreement and (or) the fulfilment of obligations under the agreement

COMMUNICATION WITH CUSTOMERS AND OTHER PERSONS, RESPONDING TO INQUIRIES SUBMITTED ON THE WEBSITE OF THE COMPANY AND/OR SUBMITTING PERSONAL OFFERS

In order to respond to inquiries about services submitted on the website of the Company and to provide you with a personal offer, we process the following personal data: name, surname, telephone number, e-mail address, IP address, and other personal data provided in the inquiry.

Purpose of data processing	Submission of a response/personal offer to the inquirer
Legal basis for data processing	Article 6(1)(a) of the GDPR – your consent as a data subject
Data retention period	3 years after submitting a response/offer

DIRECT MARKETING

To improve our services and their quality and to ensure the best possible customer experience, we may carry out various direct marketing activities. It is important for us to know what services are or may be necessary and useful to our customers. For the purpose of direct marketing, we process:

Purpose of data processing	Provision of relevant information and notifications about our services, requesting your opinion on the services provided
Legal basis for data processing	Article 6(1)(a) of the GDPR – consent of the your data subject() Article 6(1)(f) of the GDPR – for legitimate interests of the Company () (to advertise its services and provide customers and other persons concerned with relevant information about the services of the Company, to ask for opinions on the services provided)
Data retention period	5 years from the date of receipt of consent

TO WHOM CAN WE TRANSFER YOUR PERSONAL DATA?

Taking into account the basis for the provision of data and ensuring the security of the transferred data, we may transfer your personal data to third parties – service providers (data processors) who help us provide services to you and therefore need to process your personal data, and to other data recipients. The data processors we engage process personal data only in accordance with the Data Processing Agreements signed with them, which stipulate all data processing conditions and security requirements. Data processors will process personal data in accordance with our instructions and to the extent necessary to achieve the purposes of data processing. We will always be responsible for the security of your personal data, even when we entrust the processing of personal data to our data processors.

- Providers of information technology services, such as hosting services and other services for the development and maintenance of the information systems we use;
- Service providers that provide money laundering and terrorist financing prevention and fraud prevention services;
- Service providers that provide data centre and infrastructure services (e.g., server rental).

Other recipients of data to whom the Company transfers personal data process it independently, i.e., they themselves determine the purposes and means of data processing. We may transfer your personal data to the following recipients:

- Other professional service providers (auditors, other consultants, notary offices, bailiff offices, persons providing legal services to us, lawyers);
- State institutions to which we are required to provide data (the State Tax Inspectorate under the Ministry of Finance, the Bank of Lithuania, the Financial Crime Investigation Service under the Ministry of the Interior, the police and/or other law enforcement authorities, courts, etc.)
- To third parties in the case of payment initiation, account information services, transfers and other payment solutions: To the customers of the Company whose goods or services are purchased by the Payer, to banks and other financial institutions, to gambling and betting companies, to game organisation and implementation companies that use the data for personal identification and verification purposes;
- With your consent, we may also transfer your personal data to other persons.

We may also transfer or provide access to your personal data to our IT support service providers when necessary, for example, to resolve a customer service issue or to investigate and eliminate the causes of a security incident, etc.

Your personal data is usually processed within the European Union or the European Economic Area (EU/EEA). Some of our service providers and partners are located outside the European Union or the European Economic Area, so in particular situations we may need to transfer your personal data outside the EU/EEA. If, in specific cases, personal data must be transferred to third countries, when we transfer your data to third countries outside the EU/EEA, we ensure that your personal data is protected to an adequate level and that you will be able to exercise all your data subject rights and effective remedies. Your personal data may be transferred to third countries only by applying at least one of the following data transfer mechanisms and safeguards:

- Data is transferred on the basis of an adequacy decision, i.e. only to countries that, according to a decision of the European Commission, ensure an adequate level of protection;
- Data is transferred to recipients based on appropriate safeguards implemented by the Company and data recipients (processors) in accordance with contracts based on Standard Contractual Clauses approved by the European Commission;
- In specific cases, we may ask for your consent to transfer your personal data to third countries for specific purposes.

WHAT RIGHTS DO YOU HAVE?

As a data subject, you have all the rights set out in the Regulation:

- to be informed about the processing of personal data and to access the data being processed – to obtain information about whether we process your personal data and, if so, to access your personal data;
- to request the rectification of personal data if you find that the personal data we process is inaccurate or incorrect;
- to request the suspension of personal data processing, except for storage, if, after accessing your personal data, you find that the data is incorrect, incomplete, inaccurate or processed unlawfully;

- submit a request to delete personal data (“right to be forgotten”), when the request can be justified by at least one of the reasons referred to in Article 17(1) of the Regulation, except when your data must be stored on the basis of legal obligations applicable to the Company or the establishment, exercise or defence of legal claims;
- to object to the processing of personal data when such data is processed or intended to be processed for legitimate interests, including profiling, pursued by the Company, unless the data is processed for compelling legitimate reasons that override your, interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims;
- to receive personal data concerning you that you have provided to the Company, processed by automated means and based on consent or agreement, in a commonly used computer-readable format and to transfer it to another data controller (right to data portability), where this is technically feasible;
- to object to being subject to automated data processing, including profiling;
- to withdraw your consent to the processing of your personal data at any time by giving notice to the Company in the manner specified by the Company – by clicking on the link at the end of the e-mail (in case of direct marketing) or by sending your request to the Company by e-mail: asmensduomenys@neofinance.lt.
- If you believe that the actions or omissions of the Company violate your rights or the requirements of legal acts, you have the right to submit a complaint to the supervisory authority – the State Data Protection Inspectorate.

HOW CAN YOU EXERCISE YOUR RIGHTS?

You can exercise your rights yourself or through representatives by submitting a free-form request to us. You can submit your request verbally or in writing, either in person, by post or electronically (by e-mail: asmensduomenys@neofinance.lt). The request must be clear and detailed, stating your name, surname, information about the rights you intend to exercise and the scope of those rights, as well as information about how you would like to receive a response. The request must also be signed. If you submit your request electronically, the information shall also be provided electronically, unless you request otherwise in advance.

You must identify yourself by providing a document confirming your identity. If you fail to do so, we will not be able to accept your requests and the rights of the data subject will not be exercised. This provision does not apply if you are requesting information about the processing of personal data in accordance with Articles 13 and 14 of the GDPR.

When processing your request, we have the right and obligation to verify your identity, which we will always seek to do in the simplest and most convenient way for you. Your request must also contain sufficient information to allow us to reasonably verify your identity. If the request is submitted by an authorised representative, a written power of attorney and information confirming the identity of the representative must be attached to the request. If we have reasonable doubts about the identity of the individual submitting the request, we have the right to request additional information necessary to verify your identity.

We will try to review your requests and provide you with the information as soon as possible, but no later than within 30 calendar days from the date of receipt of the request. If, due to specific circumstances/the complexity of the request submitted (if it is necessary to seek assistance from data processors), or due to the number of requests being processed by the Company, the Company may not be able to process your request in a timely manner, and the processing period may be extended for up to two months, in which case we will inform you immediately. We will also inform you if we determine that you have not followed the procedure set out in this section when contacting us, indicating the deficiencies. If you do not rectify the deficiencies or inform the Company of the valid reasons why the deficiencies cannot be rectified, we will not process your request.

Requests are reviewed and information and data are provided free of charge. However, we reserve the right in specific cases either to refuse to exercise your rights (where the request is unfounded or disproportionate or is repetitive), or to charge for the provision of information and data, taking into account the administrative costs of providing the information or notifications or actions requested, administrative costs, in accordance with the requirements of legal acts and the rates set by the Company (if there is obvious abuse of your rights, unreasonably repeated requests for information, data, extracts, documents, etc.).

LINKS TO OTHER WEBSITES

Our Website may contain links to other websites, such as links to social network accounts (accounts of the Company on LinkedIn and Facebook). This Policy does not cover and does not apply to the processing of personal data by social network administrators. The Company is not responsible for the content of information provided on these websites that is not

provided by the Company, the processing of personal data, and (or) their activities. We recommend that you review and read the privacy policies and personal data processing terms and conditions of the websites that you can access from our Website using the links provided.

VALIDITY AND UPDATING OF THE PRIVACY POLICY

We regularly review our Privacy Policy and update or supplement it as necessary, taking into account changes in the applicable legal acts, the technologies we use, or our business practices. We will notify you of any updates by posting the updated Policy on our [Website](#). We recommend that you periodically review the Privacy Policy and familiarize yourself with any changes. Changes will take effect on the date they are posted on the website or on another date specified in the Policy. If you continue to use our services after the effective date of the updated Policy, we will consider that you have accepted all changes.

If you have any questions about our Privacy Policy or the processing of your personal data, please contact us by:

- E-mail: asmensduomenys@neofinance.lt ;
- By telephone: 8 700 80 075
- By post: Ukmergės St. 126, LT-08100, Vilnius, Lithuania.

This Privacy Policy was last updated and entered into force on 22 October 2025.