Privacy Notice

Version 4.00 Effective from 12.09.2022

General Provisions

Please carefully read this Privacy Notice as it sets and describes policies and practices regarding our collection, storage, processing, use, and retention of your personal data, what we do with it and why, as well as sets forth your privacy rights and Neocard role and responsibilities as controllers of your data when you use Neocard as a payment service provider, and as it becomes legally binding when you use our services.

By accessing our website www.neocard.com/Neocard App and/or using our services, you confirm that you have understood and agree to our Privacy Notice.

If you are using the services as a corporate entity, our Privacy Notice applies to individuals whose data is transmitted to us by the corporate entity.

This privacy notice is aligned with The Republic of Lithuania Legal Protection Law of Personal Data No. I-1374, Amendment No. XIII-1426 and General Data Protection Regulation. All disputes regarding the Privacy Notice provisions shall be settled by negotiation. In case of failure to resolve a case by negotiation, the dispute shall be taken to the Republic of Lithuania courts.

Definitions

Neocard or we: data controller which, alone or jointly with others, determines the purposes and means of processing personal data; where the purposes and means of such processing are determined by the Republic of Lithuania Legal Protection Law of Personal Data No. I-1374, Amendment No. XIII-1426 and General Data Protection Regulation (GDPR).

Personal data/your data: information we know about you and can be used to identify your personality.

You: an identified or identifiable individual (i.e., a data subject defined in GDPR) who is applying, accessing, or using Neocard services on your account or on behalf of a corporate entity.

Third-party: a natural or legal person, public authority, agency, or body other than you and we, who, under our direct authority, are authorised to process your data.

When and why do we collect information about you?

We may collect your different types of data from various sources. You may be:

- a visitor to our website;
- a person (or representative of a corporate entity) that has entered into (or is in the process of entering into) the Service Agreement with us or intends to use or already uses our services, including any shareholders, beneficial owners, principals, directors, and staff members accessing our website;
- a recipient of our newsletters or other marketing communications;

- a person that contacted us (or asked us to contact you) with questions, queries, requests, comments, complaints, or other communications.

What information do we collect, and from whom?

Categories of personal data that we process

We may require various types of your data, which you either provide directly to us or which we receive from third parties:

Identification and Contact Data which relates to the proper establishment of your identity:

- your name, surname;
- date of birth;
- place of birth/citizenship/nationality;
- ID information;
- actual/residence or legal/registered address, zip code, city, country;
- email address;
- mobile number;
- for corporate entities: contact person data (full name, position, phone number, and email address);
- copies of any documents you have provided for identification purposes;
- photograph/selfie of you or other data processed during the remote identification process;
- audio recordings, photos, and video recordings of you and your ID;
- residential address proof documentation;
- tax residency country/tax identification number;
- your (or your relatives') status as a politically exposed person (PEP);
- current professional or work activity;
- name of your corporate entity and its data;
- details of the device you use;
- name of your corporate entity and its data;
- any other KYC information you provide to prove you are eligible to use our services required by legislation governing the prevention of money laundering and terrorist financing.

Communication Data which related to any communication between us we store to safeguard your and our interests, conducting a quality check of the services provided by us, communication evidence, and record-keeping legitimate interests:

- communication content and metadata associated with the communication;
- email, chats, correspondence;
- record any telephone conversation between us and you regarding provisions of our services.

Transaction Data related to your transactions (including transactions into and out of your account) to provide services under the Service Agreement and keep proper records of activity:

- your Neocard card details (including card number, expiring date, CVV number, name, and billing address);

- details of your account and transaction type;
- information about your transactions (including name, address, and financial information such as your account details);
- location, date, time, amount, currencies, exchange rate, transactions details, messages sent or received with the transaction;
- details of the merchant or ATMs associated with the transaction;
- payer's and payee's name and related information;
- details of the device used to execute the transaction.

Profile Data, which is related to data directly from you or, upon your choice, from your profile to monitor and improve our website and your experience, ensure the security of our website and services, and communicate with you:

- registration information;
- communication preferences (email address, phone number, and other contact details);
- social media handles;
- feedback;
- survey/questionnaire responses.

Usage Data about your use of our website, Neocard App, and services obtained through the use of cookies, server logs, and similar technologies to have a better understanding of how you use our website, Neocard App, and services:

- *device data*: Internet Protocol (IP) address, browser/device type and version, a unique device identifier, operating system, geolocation;
- *visiting and statistical data:* referral source, timing, frequency, and pattern of your service use, length of visit, page views, download errors, length of visits to certain pages, page interaction information and methods used to browse away from the page, third party websites you access, average time spent on our website and Neocard App.

Direct Collection

We may collect and process the information you gave us when you:

- Fill up forms and applications on Neoweb banking solution or Neocard App;
- Submit your data for purposes of conclusion of a Service Agreement, registration in our system, creation of accounts, and/or linking a card;
- Sign up to your profile;
- Use of one of our services;
- Contact us (or third parties engaged by us), give us any feedback, complaint, and/or respond to our emails or surveys;
- Participate in our marketing activities, promotions, or market research;
- Visit Website, Neocard App or Neoweb banking solution.

Indirect Collection – the third parties or publicly available sources collection

We may collect your data in the course of establishing a contractual relationship or providing a service from or with the help of the categories of third parties listed below:

- Government authorities and institutions, regulators and law enforcement bodies;
- Government information systems such as registers;
- Public information sources and databases;
- Banking/financial service providers and payment networks;
- Suppliers and subcontractors that we use for the fulfilment of our commitments arising from the provision of our services to you, such as communications service providers (audio recordings, photos, and video recordings of you and your identity document), IT service providers when a provision of our service to you requires the involvement of such providers;
- Anti-fraud, risk, analytics, and compliance solution providers include but are not limited to identity verification services, fraud prevention services, and money laundering prevention services;
- Social media networks (e. g., Facebook or Google, etc.);
- Our legal, accounting, and auditing service providers;
- Third parties taking legal actions in connection with debt collection on our behalf (for instance, debt collectors, lawyers, court bailiffs, insolvency administrators, and other persons acting under the applicable laws);
- Third parties that you ask us to disclose or consent to us disclosing your data;
- Your legal representative.

Indirect Collection – Cookies and Other Technology

We may also collect non-personal information about you which does not identify you as a specific individual. Such non-personal include:

- The browser and device statistical data about the website users' browsing actions and patterns do not identify any individual;
- Cookie data include time spent on the website, visited pages, language preferences, and other anonymous traffic data.

Legal basis for using your data

The personal data collected at each stage is proportionate to the services we provide to you and the data collection purposes at the time, as we always have a lawful basis and valid legal reason for processing your data. A valid legal basis can be any of the following:

- **Contractual obligations**. We need certain obligatory personal data to enter or perform a contract with you and provide our services;
- **Legal obligation**. We are required to comply with our legal obligations;
- **Legitimate interests**. We have a legitimate reason to have it, which is reasonable for providing service to you, provided your rights do not override those reasons;
- **Consent**. Where you've agreed to use your data in a certain way.

How do we use your data?

We only use your data for the purpose we collected it or a similar, connected purpose and not processed in any ways incompatible with these legitimate purposes or legal requirements. If we ever need to use your information for an unrelated purpose, we'll inform you and explain why.

Depending on which services you use, we may process your data for the purposes listed below:

Purpose	Data	Lawful basis
Sign up with Neocard and apply for our services: – verify your identity for legal/regulatory compliance purposes; – perform screening against lists of subject to sanctions, politically exposed persons and other; – decide whether or not to approve your application; – conclusion of a Service Agreement.	▪ Identification and Contact Data ▪ Usage Data ▪ Profile Data	▪ Contractual obligations; ▪ Legal obligation (legal requirements of anti-money laundering and counter-terrorism financing and legislation related to Neocard as the payment service provider).
Provide services to you and use our services: – process your transactions; – carry out any other obligation arising from any contract entered into between you and Neocard; – perform ongoing KYC and due diligence checks; – collect fees; – resolve disputes and troubleshoot problems.	▪ Identification and Contact Data ▪ Transaction Data ▪ Communication Data ▪ Usage Data	▪ Contractual obligations (relating to any services you use); ▪ Legal obligation (relating to any services you use, legal requirements of anti-money laundering and counter-terrorism financing, and legislation pertaining to Neocard as a payment service provider); ▪ Legitimate interests (related to transaction facilitation, providing or transferring your data to our third parties who contribute to our services).
Keep our services safe and secure: – verify and confirm that you are an authorised user for security purposes; – apply "Know Your Client" and risk assessment requirements; – perform continuous and periodic monitoring of your's activity against any possible fraud, money laundering, terrorism financing, or crime risk; – understand your financial circumstances and manage fraud risks related to your Neocard account/NeoCard; – update information; – assist us with crime and fraud prevention; – manage and protect our information technology infrastructure (including video recordings on the premises managed by Neocard).	▪ Identification and Contact Data ▪ Transaction Data ▪ Communication Data Usage Data	▪ Contractual obligations (relating to any services you use); ▪ Legal obligation (relating to any services you use, legal requirements of anti-money laundering and counter-terrorism financing, and legislation related to Neocard as a payment service provider); ▪ Legitimate interests (combat money laundering and terrorist financing use of risk solution providers, development and improvement on how we deal with financial crime, maintain the integrity of our systems, and protect clients, employees, and visitors of Neocard and their property).

Informing you about our services: – changes in terms of the Service Agreement; – updating the systems; – sending system and other messages relating to the providing services.	▪ Contact Data	▪ Contractual obligations; ▪ Legal obligation.
Manage our relationship, prevent disputes, and collect evidence during relationships with you: – maintain communication; – provide customer support; – respond to your inquiries; – prevent disputes and provide evidence of communication; – protect the interests of you and/or Neocard.	▪ Identification and Contact Data ▪ Transaction Data ▪ Communication Data ▪ Usage Data ▪ Profile Data	▪ Contractual obligations (relating to your and our responsibilities); ▪ Legal obligation (relating to any services you use); ▪ Legitimate interests (to keep our records updated, improve our services, and transfer your data to our third parties who contribute to our services).
Provide you with information that we feel may interest you: – personalise marketing messages, newsletters, and offers; – measure or understand the effectiveness of advertising we serve and deliver relevant advertising to you; – provide information about our partners' promotions or offers which we think you might be interested in asking your opinion about our services.	▪ Identification and Contact Data ▪ Transaction Data ▪ Communication Data ▪ Usage Data ▪ Profile Data (only for marketing purpose)	▪ Consent; ▪ Legitimate interests (to send direct marketing and develop our services).
Improve our services and client experience: – keep our website, Neocard App and Neoweb banking solution safe and secure (including troubleshooting, data analysis, testing, research, and statistical and survey purposes); – ensure that content from the website is presented most effectively; – customising your user experience; – conduct client satisfaction surveys regarding our services; – anonymise your data for service development/improvement/testing to analyse customer behaviour; – monitor user behaviour to improve our technologies and IT infrastructure and adapt services to the devices used.	▪ Identification and Contact Data ▪ Transaction Data ▪ Communication Data ▪ Usage Data ▪ Profile Data	▪ Consent (where required by law); ▪ Legitimate interests (to develop our product offering and grow our business).
Comply with regulations and legal obligations: – comply with bookkeeping and auditing obligations;	▪ Identification and Contact Data	▪ Legal obligation (protect Neocard from legal claims, and enforce

– perform screening; – enforce our rights; – administrate debts and any disputes from the Service Agreements; – prepare anonymous reports and share data with government/regulatory authorities, law enforcement authorities, tax authorities, fraud prevention agencies.	▪ Transaction Data ▪ Communication Data ▪ Usage Data ▪ Profile Data	Neocard's legal rights, your legal rights, and the legal rights of others); ▪ Legitimate interest (protect Neocard and be a reliable market participant).

How we disclose personal data

We may disclose the data we have gathered about you with our trusted third parties when they provide services to us, to you on behalf of us, and/or under our instructions. The categories of third parties we may disclose your data with, and the purpose of such disclosure is the following:

- Banking and financial services providers that are reasonably necessary to provide our service and facilitate payment transactions or intermediaries who are an essential part of our services, including banking partners, banking intermediaries, and card association(s);
- Providers of compliance/KYC solutions and risk prevention services to fulfil our legal obligations and verify your identity and the accuracy of the data you have provided us, comply with anti-money laundering laws, protect against fraud, conduct credit checks, and confirm your eligibility to use our services;
- Card manufacturing, personalisation, and delivery companies for creating your NeoCard and delivering it to you at your requested address;
- Authorities in relation to our legal obligation or if we are permitted to do so by law, such as auditors, regulatory authorities or law enforcement bodies, courts, and other public and government authorities;
- IT vendors, cloud storage providers, and other vital operational systems providers to securely store your data;
- Neocard vendors, partners, suppliers, contractors, and professional service providers that perform certain services on our behalf / assist us in carrying out our business, such as accountants, legal consultants, audit firms, debt collection agencies, advertisers, and advertising/social networks, email service, and other IT services providers, etc;
- Analytics, customer experience support, and search engine service providers that assist us in optimising and improving our services and developing new ones;
- Third parties, if we sell or buy any business or assets, we may share your data with the prospective business owners or partners.

We do not publish a list of all the third parties with whom we may share your data, as this depends on your specific use of our services. If you want further information, you can request this by writing to **support@neocard.com**

Mainly our third parties are located in the European Economic Area (EEA). We may transfer your data outside the EEA where the transfer is necessary for the conclusion or execution of a Service Agreement. If we share your data, we will be performed it under the regulatory enactments and under certain circumstances being in force in the EU in the area of data protection to ensure that both ourselves and our third parties take adequate and appropriate technical, physical, and organisational security measures to protect your data, in line with this Privacy Notice.

Profiling

The profiling we carry out is due to our legal obligations to comply with laws relating to risk management and fraud (anti-money laundering and sanctions checks, address check, monitoring of your account to detect financial crime).

How do you use my data for marketing?

You have the right to ask us not to process your data for marketing purposes. We will inform you before collecting your data if we intend to use your data to get your consent to send marketing messages.

We use your data to personalise marketing messages about our products and services so they are more relevant and interesting to you (where allowed by law).

Your rights

You have certain rights concerning the way we treat your data. By contacting us at **support@neocard.com** and sending your request, you may exercise any of your rights about your data as the data subject, including the following:

- **Access** your data and receive information regarding your data that we process, the purposes of the processing, the recipients to whom the personal data have been or may be provided, and the rationale for such processing. The first copy will be provided free, but additional copies may be subject to a reasonable fee.
- **Rectify** the data we have about you if you believe it is incorrect, incomplete, or inaccurate.
- **Delete** your data or cease the processing of your data when it is no longer needed for the purposes for which they were collected, your data processed illegally, you withdraw consent to the processing of your data or didn't provide such consent, except the obligations required to us by legislation. This right may be subject to certain exemptions in situations to protect our or third parties' legitimate interests, comply with governmental and regulatory obligations, resolve disputes, troubleshoot problems, or enforce any agreement you have entered into with us. We will inform you accordingly if we are not able to fulfil your request or make the immediate erasure of your data.
- **Restrict** the processing of your data **or object** to our processing of your data for direct marketing. If you believe your information is incorrect or we use your data unlawfully, you have the right to ask us to stop the processing. You may also object to our processing where you believe some circumstances would make such processing unlawful.
- **Withdraw** previously given consent for processing your data at any time. Your withdrawal will not affect the lawfulness of data processing before the withdrawal. We will inform you (before collecting your data) if we intend to use your data for such purposes or if we intend to disclose your information to any third party.
- **Transfer your data** to you or directly to another controller company in an easily readable format, and we will comply with such request, provided that the personal data processing previously carried out by us was based on your consent or was necessary for the performance of a Service Agreement and where it is technically feasible.
- In case you have not received a satisfactory reply or solution from us, you have the right to **make a complaint** to your supervisory data protection authority regarding the processing of your data or if there is a problem with

the way we are handling your data or the personal data is processed in violation of your rights and legitimate interests. In Lithuania, that is the State Data Protection Inspectorate: https://vdai.lrv.lt/en/.

The person submitting the request must indicate their full name and sign the request with a qualified electronic signature. When you exercise one of your rights, it may take up to one month to make changes and respond.

How do we protect your data?

When we store or disclose your data, we take all reasonable contractual, legal, technical, and organisational measures to ensure that this data is processed with adequate protection and follows applicable legislation. As a result, the ability of third parties to use your data is limited, and they can't use your personal data for purposes other than providing services to us. However, in some cases, third parties may process your data as independent data controllers.

The transmission of data via the internet is not completely secure, and we cannot guarantee the security of your data during transmission; we are doing our best to protect your data once we have received your data. We use strict procedures and security features to prevent any unauthorised access, copying, accidental or unlawful erasure, or disclosure.

We are not responsible for protecting your privacy on websites of any third parties, even if you access such websites through links provided on our website. Therefore, please check these policies before submitting personal data to these websites.

We do not sell or rent information provided by our clients to any third party. Any user statistics are provided in the aggregate only and do not include personally identifiable information about any individual or corporate client.

How long do we store your data?

We will store your data for the period necessary to fulfil the purposes for which we collected the data unless a more extended keeping period is required for legal, regulatory, or operational reasons or to protect our or any third party's legitimate interests.

If we use your data for more than one purpose, we will store it until the purpose with the latest period expires; but we will stop using it for the purpose(s) with a shorter period once that period expires. We will typically keep your data for no longer than 8 (eight) years following the end of the provision of services, and such period for which we may retain data about you will depend on:

- the purposes for which we collected the data,
- whether you have requested deletion of the data or withdraw your consent to the retention of your data; and
- whether we have reasonable grounds for believing that we need to retain your data for legal proceedings.

When your data is no longer needed, we either completely anonymise the data to use the anonymised information or securely delete the data.

Cookies

The cookies are a small amount of data, often including a unique anonymous identifier sent to your browser from a website's computer and then stored on your hard drive.

We use cookies to remember and identify a connection session and distinguish you from other website visitors. The cookies do not collect your personal data and last until you close your browser and are used to remember your choices or, for statistical purposes, under your consent.

Using cookies helps us ensure the website's technical functionality and provides a good experience while browsing the website.

For additional information on cookies, please see our **Cookie Policy**.

Use of services by minors

Our services are not directed to persons under 18, and we kindly ask such persons not to disclose their data to us.

Changes to our privacy notice

As data protection is Neocard's ongoing responsibility, we regularly review this Privacy Notice and reserve the right to modify it at any time following applicable laws and regulations. Accordingly, an updated version of our Privacy Notice will take effect immediately upon its publication on our website.

How to contact us?

If you wish to contact us regarding this Privacy Notice, exercise your right, or make a complaint, please use the email address **support@neocard.com** indicating your name, surname, and request details or the following address:

UAB NEOCARD Topoliu str. 24A-2, Nemezio village, Vilnius district, LT-13262, Lithuania