Privacy Notice

Version 3.1 Effective from 04.07.2022

Definitions

The “Institution” shall mean the UAB “NEOCARD“.

The “Controller” shall mean the natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Law. In this instance, the Institution is Data Controller.

The “Data Processor” shall mean a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

The “Data Subject” shall mean the individual in relation to which Institution is holding information about; in the context, this is employees, partners, customers, other individuals to whom Institution renders services.

The “Law” shall mean The Republic of Lithuania Legal Protection Law of Personal Data No. I-1374, Amendment No. XIII-1426 valid from July 16, 2018, and General Data Protection Regulation (EU) 2016/679 of 27.04.2016.

General Provisions

This privacy statement sets out the privacy policy of platform UAB “NEOCARD” (hereinafter «Institution», «we») which is located at site https://www.neocard.com/ (hereinafter «the Website») and any services or features which are available to you from this Website.

We are committed to protect your Personal Data and respect your privacy. This privacy notice (together with the General Electronic Money and Payment Service Agreement) sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us and what choices you have about your personal data. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it.

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.

What Information Do We Collect?

We collect personal information about you when you use our products or services, or deal with us in some way.

We collect information about you from a variety of sources, such as:

- Applications, personal financial statements, and other written or electronic communications reflecting information such as your name, address, identification number, occupation, assets, and income.
- Transactional account history including your account balance, payment records, and credit card usage.
- Information received from third parties, (e.g. government, regulatory, or credit agencies).

This includes collecting information when you:

- Contact us — for example, when you sign up, fill in an application or order form, give us feedback or make a complaint.
- Use our products or services – for example, when you perform transactions, use your debit or credit card or make exchange operations.
- Visit our website or use our mobile apps.

The information we collect from you may include:

- Login credential information – including your email address and phone number.
- Information about your identity data — including your name, date of birth and other ID information.
- Information about contact data may include your declared and actual address of residency, telephone number, email address.
- Due diligence information – including Know your customer, Anti-Money-Laundering and other customer registration information.
- Other personal information, such as details of your interactions with us.
- Information about transaction data may include financial, transaction information, card details.
- When you visit our website or use our mobile apps we collect usage data —your location information, IP address, browser type and version, operating system and any third-party sites you access.

What are Your Rights?

You have rights to transparent information, communication and modalities for the exercise of your rights as the Data Subject under the Law. Your principal rights under the Law are:

- the right to be informed;
- the right to access;
- the right to rectification;

- the right to erasure;
- the right to restrict processing;
- the right to object to processing;
- the right to data portability;
- the right to complain to a supervisory authority; and
- the right to withdraw consent.

You have the right to be informed about the collection and use of personal data. The information must be concise, transparent, intelligible, easily accessible, and written in clear and plain language.

You have the right to request details of personal information which we hold about you under the Law, this includes access to the personal data, together with certain additional information. Additional information includes details of the purposes of the processing, the categories of personal data. The rights and freedoms of others are not affected.

You have "the right to be forgotten", to the erasure of your personal data without undue delay. It applies to the following circumstances:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- you withdraw consent to consent-based processing;
- you object to the processing under certain rules of applicable data protection law;
- the processing is for direct marketing purposes;
- the personal data have been unlawfully processed.

However, there are exclusions of the right to erasure. The general exclusions include where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; or for the establishment, exercise or defence of legal claims.

In some circumstances you have the right to restrict the processing of your personal data. Those circumstances are: you contest the accuracy of the personal data; processing is unlawful but you oppose erasure; the personal data is no longer needed for the purposes of the processing, but you require personal data for the establishment, exercise or defence of legal claims; you have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store your personal data.

You have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

To the extent that the legal basis for our processing of your personal data is consent; or that the processing is necessary for the performance of an agreement to which you are a party or in order to take steps at your request prior to entering into a contract, and such processing is carried out by automated means, you have the right to receive your personal data from us in a structured, commonly used and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.

If you consider that processing of your personal information infringes data protection laws, you have a legal right to lodge a complaint with a supervisory authority responsible for data protection. You may do so in the EU member state of your habitual residence, your place of work or the place of the alleged infringement.

To the extent that the legal basis for our processing of your personal information is consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

You may exercise any of your rights in relation to your personal data by written notice to us.

How Do We Collect Your Information?

Direct Collection

- We collect much of the information listed above directly from you when you submit it on our website or through our mobile application. This includes information such as contact information, registration information and service inquiries.
- If you do not want to share your information, you can choose not to participate in a particular service or activity.

Indirect Collection – Cookies and Other Technology

As part of offering and providing personalized services, the Institution uses cookies and local device storage. We may use these technologies to:

- Provide you with personalized content based on your use of the Website
- Enable you to more easily use the Website by remembering and using contact information, purchasing information, and registration information
- Evaluate, monitor and analyze the use of the Website and Institution mobile application and their traffic patterns to help improve the Website and services
- Assist us with ad reporting functions such as learning which ads are bringing users to the Website

The types of technologies we use include:

- ***Cookies***. A cookie is a small amount of data that is sent to your browser from a Web server and stored on your computer's hard drive. Cookies enable us to identify your browser as a unique user. Cookies may involve the

transmission of information from us to you and from you to us. Cookies may also be used by another party on our behalf to transfer information to us in accordance with their privacy policy. Some cookies are "persistent cookies". They are used by us each time you access our website. Other cookies are called "session cookies". “Session cookies”, also called “session variables”, are used only during a specific browsing session and expire after a pre-determined amount of time. We may use a session cookie, for example, to remember that you have already navigated through a particular menu. We may also use "analytics cookies" that allow web analytics services to recognize your browser or device and, for example, identify whether you have visited our website before, what you have previously viewed or clicked on, and how you found us. This information is provided anonymously for statistical analysis only. Analytics cookies are usually persistent cookies. You may disable browser cookies in your browser or set your browser to warn you when a cookie is being sent. You may lose some features or functionality when you disable cookies. Remember, also, that disabling cookies is browser-specific.

- ***Log Files.*** Like most standard website servers, we use log files. Log files track Internet protocol (IP) addresses, browser type, Internet service provider (ISP), referring/exit pages, platform type, date/time stamp, and a number of clicks. We utilize this information to analyze trends, administer the site, prevent fraud, track website navigation in the aggregate, and gather broad demographic information for aggregate use.

How Do We Use Your Information?

We are careful about how we use your information. We use it to deliver our products and provide our services. We also use your information for other reasons, such as to better understand you and your needs and to let you know about other products and services you might be interested in.

We collect, use and exchange your information for the following purposes:

Provision of financial services

1. Customer identification;
2. Account servicing/ provision of the payment services:
    - Payment service provision;
    - Issuance and servicing of payment cards / credit cards;
3. Providing remote financial institution services:
    - Provision of EMI services:
    - Provision of mobile application services;
    - Using cookies;
4. Enforcement of statutory obligations:

- Know-Your-Customer research, incl. identification of the customer, identification of the beneficial owner and clarification of a politically significant person;
- Public Institutions / Investigations, etc. execution of law enforcement requests;
- Fulfilment of AML law requirements, such as suspicious and unusual transaction tracking system maintenance and reporting;
- Control service reporting.

5. Customer support:
   - Provision of general information via telephone;
   - Website online request form fulfilment;
6. Marketing purposes:
   - Customer group evaluation and research;
   - Sending commercial notices;
   - Organization of customer events;
   - Addressing potential clients;
   - Using cookies.

We shall use the personal data in compliance with the Law, and the confidentiality obligation contained in the General Electronic Money and Payment Service Agreement, and only use and retain such data as far and as long as this is necessary for the purposes of Institution utilization, rendering of services on the Website and for keeping customers informed of Institution services.

In addition, our mobile application will collect and track information regarding the mobile experience - such as your phone model, the duration and frequency of your usage sessions, information regarding application crashes, the particular screens you choose to view, etc.

Disclosure of Information

We will not disclose any of your personally identifiable information except when we have your permission or under special circumstances, such as when we believe in good faith that the Law requires it or under the circumstances described below.

These are some of the ways that your information may be disclosed

Service Providers

We occasionally hire other companies to provide limited services on our behalf, including Website development and operation, sending postal mail or email, analyzing website use, processing payments, processing data. We will only provide those companies the information they need to deliver the service, and they are contractually prohibited from using that information for any other reason.

To make an informed decision on whether to provide your personal data to the Institution using this website, we need to make you aware of organizations that act as Data Processors for us in the provision of our services to you:

- **UAB "FININBOX"** – Banking Information System FORPOST for management of the Customer's information flow and record keeping;
- **Central Bank of Lithuania** - payment service system provider, to send and receive SEPA payments;
- **CENTROlink** – a payment system operated by the Bank of Lithuania, providing the gateway to the Single Euro Payments Area (SEPA);
- **UAB "Identifikaciniai projektai"** – personal identification service provider;
- LexisNexis Risk Solutions (Europe) Ltd. - Anti-Money Laundering solutions;
- Mastercard International Incorporated – MasterCard principal license;
- **SIA Decta** – card payment processing services;
- **EVRY Card Services Oy** – card issuing services;
- **iSPIRAL IT SOLUTIONS LTD** – Onboarding/KYC/AML/FRAUD solution.
- **iSPIRAL IT SOLUTIONS LTD** – Onboarding/KYC/AML/FRAUD solution.
- **INTERCOM Inc**. – customer support solution.
- Webflow Inc. – landing page hosting solution.

Data in the Aggregate

We may disclose "blinded" aggregated data and user statistics to prospective partners and other third parties. Blinded data is data that does not identify an individual person.

Other

We also may disclose your information in special cases, for example, when we believe that we must disclose information to identify, contact or bring legal action against someone who may be violating our Terms of Service Agreement, or may be causing injury to or interference with our rights or property, other website users or customers, or anyone else who may be harmed by such activities. We may disclose or access account information when we believe in good faith that

the law requires it and for administrative and other purposes that we deem necessary to maintain, service and improve our products and services.

As we continue to develop our business, we may buy or sell businesses or assets. In such transactions, confidential customer information generally is one of the transferred business assets. In the event of a transaction involving the sale of some or all of the Institution's business, customer and site visitor information may be one of the transferred assets and may be disclosed in connection with negotiations relating to a proposed transaction. In such case, the transferred information may become subject to a different privacy policy.

Security

How do we keep your information safe?

We use multiple security measures to ensure the confidentiality of your information. We aim to only keep your information for as long as we need it.

We store your hard copy and electronic records in secure buildings and systems. Access to your personal information is permitted only for Institution authorized employees.

System security

When you log into our Website or apps, we encrypt data sent from your computer to our systems so no one else can access it. We have firewalls, intrusion detection and virus scanning tools to stop viruses and unauthorized people from accessing our systems.

We use Secure Sockets Layered (SSL) technology to ensure that your information is fully encrypted and sent across the Internet securely.

We use encryption technology in accordance with ISO 27001 and PCI-DSS requirements for payment card numbers, passwords, and registration information.

Every session required for Two Factor Authentication, is an extra layer of security that requires not only a password and username on your login at the Institution.

How can you control your personal information?

We offer our customers choices for the collection, use and sharing of personal information. You may contact us at support@neocard.com if you wish to edit your private information and we will use commercially reasonable efforts to accommodate your request.

If you believe that any inaccurate or inappropriate information has been obtained or provided to others through your use of this website, you should contact a representative of tht Institution via email: support@neocard.com or at the branch located on P.Babickio g. 22C, LT-11311, Vilnius, Lithuania, I-V from 9 a.m. to 5 p.m. Make sure to have your ID document with you.

How to Access Your Personal Information?

To get access to your personal data processed by Institution, please submit a request via email support@neocard.com or at the branch located on P.Babickio g. 22C, LT-11311, Vilnius, Lithuania, I-V from 9 a.m. to 5 p.m. Indicate your full name and attach a copy of your ID document.

We will provide the required data or the reason for refusal to provide such data within the period set by legislation.

How do We Protect Financial-related Information?

Keeping your personal financial information private is very important to us. As a matter of policy and long-time business practice, we do not sell information provided by our users. Any user statistics that we may provide to prospective partners regarding financial matters are provided in the aggregate only and do not include any personally identifiable information about any individual user or corporate user.

What security precautions are in place to protect against the loss, misuse, or alteration of my information?

Remember to sign out of your account and close your browser window when you have finished your work. This is to ensure that others cannot access your account by using your computer when you are away from it. Because information sent through the Internet travels from computer to computer throughout the world, when you give us information, that information may be sent electronically to servers outside of the country where you originally entered the information.

Unfortunately, no data transmission over the Internet can be guaranteed to be 100% secure. Information that you disclose by use of the Website (as with any site that is non-secure), by posting a message or using e-mail, potentially could be collected and used by others. This may result in unsolicited messages from third parties or use of such information by third parties for their own purposes, legal or illegal. As a result, while we strive to protect your personal information, we cannot ensure or warrant the security of any information you transmit to us or from our services, and you do so at your own risk. Once we receive your transmission, we use commercially reasonable efforts to ensure its security on our systems.

Do You Get Informed About Personal Data Breach?

When do we need to tell you about personal breach?

In the case of a personal data breach, we shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify. If a breach is likely to result in a high risk to the rights and freedoms of individuals, we must inform you directly and without undue delay.

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

How to Contact Us?

You can contact us any time to exercise any of your rights in relation to your personal data or if you have any additional questions about Privacy collection and storage of data by contacting us at support@neocard.com. The person submitting the request must clearly indicate his/her full name and add a copy of his/her personal identification document.