# PRIVACY POLICY

## Purpose of the Privacy Policy

The Privacy Policy is meant for use by Customers of Company. This Privacy Policy describes how the Company's Customers personal data is collected and processed.

The company is compliant with the applicable Lithuanian and International laws for the Prevention of Money Laundering and Terrorist Financing, the GDPR as well as repealing Directive 95/46/WE (general regulation on data protection) and other relevant binding provisions of law applicable in Lithuania. This policy shall be regulated by applicable laws and regulations of Lithuania, General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR).

This Privacy Policy aims to provide Company's Customers with information on what type of information Company collects, how it is used and the circumstances where it could be shared with third parties.

As a general rule, the Customer data is processed within the European Union/European Economic Area (EU/EEA), but in some cases it is transferred to and processed in countries outside the EU/EEA.

The transfer and processing of Customer data outside the EU/EEA can take place provided there are appropriate safeguards in place and the actions are made based on a legal basis only.

Upon request, the Customer may receive further details on Customer Personal data transfers to countries outside the EU/EEA.

## Personal data and rights and obligations of the Company

The Company shall collect information necessary to fulfill legal obligations for the provision of services and to improve Company services.

The Company may collect personal information about the Customer from third parties, service providers that are assisting Company in providing services and helping Company to offer services effectively. Customer's Personal data will be used for specific, explicit and legitimate purposes according to the Lithuanian and International laws for the Prevention of Money Laundering and Terrorist Financing, as well as in order to enhance Customer support and also is used to verify Customer's identity for Due Diligence purposes, to manage Customer's account with the Website Platform.

The Company may collect personal information about the Customer in order to:

-comply with legal requirements for anti-money laundering and counter-terrorist financing
-process Customer's transactions;
-provide Customers with post-transaction information;
-inform Customers of additional products and/or services relevant to Customer's profile;
- to produce analysis and statistical data which will help the Company improve its products and services, and also for the Website Platform enhancement purposes.
- fulfill the obligations and to provide the Customer with the services for which the Company have received the Customer's consent.

Company may collect the following Personal Data:

- information (name, surname, nickname, email, address and other information) that is necessary to identify Customer and to prevent using account by unauthorized parties;
- data about Customer account (we may create a specific ID for you when you use the Services);
- data for analytics purposes;
- profile and usage data;
- data about Customer device, such as manufacturer, operating system, CPU, RAM, browser type and language;
- data about Customer device, such as manufacturer, operating system, CPU, RAM, browser type and language;
- Customer messages and feedback about experience with Company;
- data (such as Customer nickname, profile picture) received if Customer link a third-party tool with the Service (such as Facebook, Google, etc.);
- details of orders (amount spent, date, time, vouchers or offers used);
- data collected with cookies and other technologies;
- data to fight fraud and data required by anti-money-laundering provisions;
- payment and transaction data;
- data about Customer account (we may create a specific ID for you when you use the Services);
  IP address and unique mobile device identification numbers (such as Customer device ID, advertising ID, MAC address);
- precise geolocation data (GPS);
- other Personal data Customers have sent.

The Company is obliged to:

- inform its Customers of any material change to this Privacy Policy;
- at the request of the Client, immediately stop processing personal data for marketing purposes;
- stop processing personal data in accordance with the requirements of national and international law, as well as at the request of the relevant state authorities;
- refrain from transferring or disclosing personal data of Clients to third parties, except when such disclosure is required in accordance with the law, by a court decision, at the request of a state authority, or for other reasons provided for by the norms of international and national law.

The Company services are not provided to the people younger than eighteen (18) years of age. The Company does not intend to collect Personal data from such people. If the Customer is under 18, please do not use the Services and do not send any Personal data to the Company. In the event that a Company learns that they have collected Personal data from a person under age 18, will delete that Personal data as quickly as possible.

## Collecting and processing

Company and any third parties acting on Company's behalf for the purpose of collecting, storing and processing personal data may collect, process and store personal data provided by the Customer.

For the purpose of processing and the storage of personal data provided by the Customer in any jurisdiction within the European Union or outside of the European Union, the company can confirm this will be done in accordance with applicable laws.

## Safeguarding legitimate interests

Company processes personal data to safeguard the legitimate interests pursued by Company or by a third party. A legitimate interest is when a Company has a business or commercial reason to use Customer's Personal data. Even then, it must not unfairly go against what is right and best for the Customer.

Examples of such processing activities include:

- initiating court proceedings and preparing defense in litigation procedures;
- means and processes to provide for the Company's IT and system security, preventing potential crime, asset security, admittance controls and anti- trespassing measures;
- measures to manage business and for further developing products and services;
- the transfer, assignment and/or sale to one or more persons and/or charge and/or encumbrance over, any or all of the Company's benefits, rights, title or interest under any agreement between the Customer and the Company.

## Marketing Purposes

The Company may process Customer's Personal data to deliver any news , analysis, research, reports, campaigns and training opportunities that may interest the Customer, to their registered email address.

The Personal data that Company processes for this purpose consists of information Customers provide to the Company and data Company collects and/or infers when Customer uses services of the Website Platform, such as information on Customer's transactions. Company studies all such information to form a view on what is needed or what may be of an interest to Customers.

In some cases, profiling may be used. Profiling is a process when Customer's data is being automatically processed with the aim of evaluating certain personal aspects and to further provide Customers with targeted marketing information on services.

The Customer always has the right to change and cancel the option if no longer wishes to receive marketing related emails to Customers provided email addresses.

Customers have the right to object at any time to the processing of Customer's Personal data for marketing purposes or unsubscribe to the provision of marketing related emails by the Company, by contacting at any time Company's Customer support department via the following ways:

- By Email: support@onchainpay.org
- Customer support via the Website Platform

## Authorized Processor

The GDPR sets out what needs to be included in the contract which the Company has adhered to, obligations of all relevant parties, for example, are:

- third parties must only act on the written instructions of the Company (unless required by law to act without such instructions);
- ensure that processing the Personal data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- the rights of Customers will not be impaired in meeting with GDPR requirements;
- the security of processing, the notification of Personal data breaches and Personal data protection impact assessments will not be impaired;
- deletion or return of all Personal data as requested at the end of the contract.

Company has a regulatory obligation to supervise and effectively oversee the outsourced functions and to act appropriately when it determines that the service provider is not performing the said functions effectively and in accordance with the applicable legislation. Company may use or disclose Personal data without Customer's consent only in certain circumstances:

- if required by law or by order of a court, administrative agency, or other government entities;
- if there are reasonable grounds showing disclosure is necessary to protect the rights, privacy, property, or safety of Customers or others;
- if believe the Personal data is related to a breach of an agreement or violation of the law, that has been, is being, or is about to be committed;
- if it is necessary for fraud protection, risk reduction, or the establishment or collection of funds owed to us;
- if it is necessary to enforce or apply the Terms and Conditions and other agreements, to pursue remedies, or to limit damages to Company;
- for other reasons allowed or required by law;
- if the Personal data is public.

When the Company is required or permitted to disclose personal data without consent, the Company will not disclose more Personal data than necessary to fulfill the disclosure purpose.

The Company informs all Customers to maintain confidentiality and not to share with others its Customer names and private passwords or as provided by the Company. The Company bears no responsibility for any unlawful or unauthorized use of Customers' Personal data due to the misuse or misplacement of Customers' access codes (i.e. passwords/credentials), negligent or malicious, however conducted.

## Period

The Company will keep Customers personal data for:

As long as a business relationship exists with the Customer or once the business relationship with Customers has ended, the Company is required to keep Customers Personal data for a period of five years to meet regulatory and legal requirements. This period may be extended. When Company no longer needs Customer's Personal data, Company will securely delete or destroy it and.

## Customer's rights

Customer has the right to request copies of his/her Personal data. Information of Personal data must be provided without delay and at the latest within one month of receipt. The Company will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, the Company will inform Customers within one month of the receipt of the request and explain why the extension is necessary.

Company must provide a copy of the information free of charge. However, the Company can charge a "reasonable fee" when a request is manifestly unfounded or excessive, particularly if It is repetitive.

The fee, if applied, will be based on the administrative cost of providing the information and for delivery expenses, if Customer requests to deliver this information in hard copy. If at any time Company refuses to respond to a request, Company will explain why to the Customer, informing Customer of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

## Miscellaneous

The Company has implemented security measures to ensure the confidentiality of Customers personal data and to protect data from loss, misuse, alteration or destruction. The security measures in place will, from time to time, be reviewed in line with legal and technical developments. Unfortunately, the transmission of information via the Internet is not completely secure. Unauthorized entry or use, hardware or software failure, and other factors, may compromise the security of Customer Personal data at any time.

Among other practices, Customer's account is protected by a password for Customer's privacy and security. Customers must prevent unauthorized access to Customer's account and Personal data by selecting and protecting Customer's password appropriately and limiting access to Customer's computer or device and browser by signing off after finishing accessing Customer's account.

Transmission of Personal data and information via regular email exchange is not always completely secure. The Company however exercises all possible actions to protect Customers' Personal data, yet it cannot guarantee the

security of Customer data that is transmitted via email; any transmission is at the Customers' own risk. Once the Company has received the Customer Personal data it will use procedures and security features in an attempt to prevent unauthorized access.

When Customers email the Company or using the Contact form feature, a Customer may be requested to provide some additional Personal data, like their name or email address. Such data will be used to respond to query and verify Customer's identity. Emails are stored on Company's standard internal contact systems which are secure and cannot be accessed by unauthorized external parties.

## Complaints

Any concerns and/or requests can be send:

Email: support@onchainpay.org

Customer has the right to be confident that Company handles Customer's Personal data responsibly and in line with good practice. If a Customer has a concern about the way the Company is handling Customer's Personal data, or for example if a Customer feels we may not be;

- keeping Customer's Personal data secure;
- holds inaccurate Personal data;
- has disclosed Personal data;
- is keeping Personal data about Customer for longer than is necessary;
- has collected Personal data for one reason and is using it for something else.

Company takes all concerns seriously and will work with Customer to resolve any such concerns.

Customers' written requests may be required for security reasons. We may decline the request, if there are reasonable grounds to believe that the request is fraudulent, unfeasible or may jeopardize the privacy of others.

## Changes in Privacy Policy

The Company reserves the right to modify the Privacy Policy at any time at the Company's sole discretion. If any changes are made, the Company shall notify Customer accordingly. The Company encourages Customers to review this Privacy policy occasionally so as to always be informed about how the Company is processing and protecting Customers Personal data. The Company will review the Privacy Policy at least annually. A review will also be carried out whenever a material change occurs that affects the ability of the Company to continue to the best possible result for the execution of its Customer Orders on a consistent basis using the venues included in this Privacy Policy. If the Customer continues to use the Services, the amended Privacy Policy has legal force the Customer actions will constitute acceptance of the amendments.

The Company will inform its Customers of any material change to this Privacy Policy by posting an updated version of this Privacy Policy on its Website and/or to Customer email.