PRIVACY POLICY

In the present privacy policy (**„Policy“**) we provide the main information on how we, electronic money institution **UAB „NS Pay“** (**„Data Controller“** or **“we”**), process personal data of our customers, their representatives, other persons associated with our activities or the provision of our services, and visitors to our website https://www.nspay.eu/ (**„Website**“).

Please be informed that your personal Data Controller is:

UAB „NS Pay“	
Legal entity code:	305652931
Registered office address	A. Domaševičius St. 9, Vilnius
Phone number	+370 682 22504
E-mail	info@nspay.lt

Should you have any questions regarding the protection of your personal data or this Policy, we recommend that you contact us immediately using the contact details above.

Please be informed that when processing your data we also adhere to:

(i) the General Data Protection Regulation („**GDPR**“);

(ii) the Law on the Legal Protection of Personal Data of the Republic of Lithuania;

(iii) the Law on Electronic Communications of the Republic of Lithuania; and

(iv) other applicable legal acts as well as the instructions and recommendations of the supervisory authorities.

When processing your personal data, we comply with the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation and data accuracy. We also have security measures and procedures in place to protect your personal data against unauthorised access, disclosure, loss, alteration, destruction or other unlawful processing.

1. Definitions

1.1. In this Policy, capitalised terms shall have the meanings set out below, unless the context otherwise requires:

1.1.1. **Personal Data** – any information which can be used to identify, directly or indirectly, a natural person, as well as any information about a natural person who has already been identified;

1.1.2. **Data Subject** – a natural person who is a visitor to the Website, a customer of ours, a sender of enquiries to us, or any other person in connection with our business and (or) the services we provide;

1.1.3. **Processing** – any operation performed on Personal Data, including, but not limited to, collecting, recording, organizing, storing, modifying, accessing, using, etc.

1.2. Other terms used in the Policy shall have the same meaning as defined in the GDPR and other applicable law.

2. Purposes of Processing Personal data

2.1. We process your Personal Data for the following purposes:

2.1.1. remote identification;

2.1.2. continuous monitoring of business relationships;

2.1.3. prevention of money laundering and terrorist financing;

2.1.4. enforcement of international sanctions;

2.1.5. implementation of the requirements of legislation on the prevention of tax evasion;

2.1.6. the provision of our services;

2.1.7. the conclusion and performance of a contract;

2.1.8. the prevention of payment fraud;

2.1.9. improving the quality of our services;

2.1.10. preventing, limiting and investigating any abuse, misuse or interference with our services, or bringing, enforcing and defending legal claims;

2.1.11. direct marketing;

2.1.12. to respond to your enquiries;

2.1.13. compiling statistics and (or) reports.

2.2. In each case, the basis, scope, retention periods and other circumstances relating to the processing of your Personal Data are defined below in this Policy.

3. The categories of Personal Data processed

3.1. The Personal Data processed shall be divided into the following groups:

Category of Personal Data	Personal Data Processed
Main Personal Data	Name, double name, surname, gender.
Personal identification data	Name, double name, surname, personal identification number, date of birth, citizenship, details of your identity document and copies of it, photograph, biometric data (such as a picture of your face ("selfie") and a video), permanent residence permit.
Contact details	Telephone number, email address, residential address, registration address or correspondence address.
Payment data	Sender/receiver of funds, account number, purpose of payment, payment amount and currency, payer identification code, payment instruments and the actions taken using them, etc.
Financial data	Data on available property, transactions, loans, income, liabilities, accumulated assets.
Data relating to your credibility and performance evaluation	Payment transaction data, data necessary for us to take the necessary measures to prevent money laundering and terrorist financing and to enforce international sanctions, including to determine the purpose of the business relationship with the customer and whether the customer is a politically exposed personas well as the source of the origin of the assets, data on the customer's counterparties and business activities, etc.
Data obtained and (or) generated in compliance with the requirements of applicable legislation	Data that we are required to provide to public authorities, such as tax authorities, courts, other enforcement authorities, including data on income, financial obligations, available property, etc.
Data about your actions on the Website and (or) in your personal account	Information about your actions on the Website, related technical information, the IP address used at the time of connection of the Internet user, the version of the operating system and the parameters of the device you use to access the content/services; login information - the

	timing and duration of the use of your session; the time limits of the queries you enter on the Website, etc.
Correspondence data	Letters, emails and other forms of communication and their content.
Other data	Data on participation in companies and other types of legal entities, data on directors and other persons with decisive voting rights or representatives of companies that use or intend to use our services, as well as information on their beneficial owners and contact details of the representatives of companies that use or intend to use our services, information that the customer has been assigned to a certain risk level, the location of the transaction, the IP address, the location of the login etc.

4. Processing of your Personal Data

4.1. Below are the main purposes, legal bases and categories of processed Personal Data of our customers. We inform you that below is general information about what Personal Data we can process, but depending on individual circumstances, the scope of Personal Data Processing may vary.

The purpose of Personal Data Processing	Legal basis for Processing Personal Data	Category of Personal Data
Remote identification	Your consent	Main Personal Data, Contact details.
Continuous monitoring of business relationships	Legal obligation	Payment data, Data relating to your credibility and performance evaluation.
Prevention of money laundering and terrorist financing	Legal obligation Public interest	Main Personal Data, Personal identification data, Contact details, Payment data, Financial data, Data relating to your credibility and performance evaluation, Data about your actions on the Website and (or) in your personal account, Correspondence data, Other data.
Enforcement of international sanctions	Legal obligation Public interest	Main Personal Data, Personal identification data, Contact details, Payment data, Financial data, Data relating to your credibility and performance evaluation, Data about your actions on the Website and (or) in your personal account, Correspondence data, Other data.
Implementation of the requirements of legislation on the prevention of tax evasion	Legal obligation	Personal identification data, Contact details, Data obtained and (or) generated in compliance with the requirements of applicable legislation, Other data.
The provision of our services	Performance of the contract	Main Personal Data, Contact details, Payment data, Data about your actions on the Website and

		(or) in your personal account, Other data.
The conclusion and performance of the contract	In order to take steps prior to entering into the contract and performance of the contract	Main Personal Data, Personal identification data, Contact details, Payment data, Financial data, Correspondence data, Other data.
The prevention of payment fraud	Legal obligation Legitimate interest	Payment data, Data about your actions on the Website and (or) in your personal account, Other data.
Improving the quality of our services, including the handling of complaints and/or claims made by you	Legal obligation	Main Personal Data, Contact details, Data about your actions on the Website and (or) in your personal account, Correspondence data, Other data.
Preventing, limiting and investigating any abuse, misuse or interference with our services, or bringing, enforcing and defending legal claims	Legal obligation Legitimate interest	Main Personal Data, Personal identification data, Contact details, Payment data, Financial data, Correspondence data, Other data.
To respond to your enquiries	Your consent Performance of the contract	Main Personal Data, Contact details, Correspondence data.

4.2. We also collect data about persons related to you, such as legal representatives (whether acting under a power of attorney or otherwise). In the event that you provide us with the data of other persons related to you, you are obliged to inform them of our Processing of their Personal Data, and you are obliged to make them aware of this Policy.

5. Processing of Personal Data for direct marketing purposes

5.1. In the event that you are a customer of ours, we may use your Contact details for the purpose of direct marketing of similar services by providing you with a clear, free and easy-to-use opportunity to object to or withdraw such use of your Contact details for the purposes set out above and provided that you have not objected to such use initially.

5.2. In all other cases, we may use your Contact details for direct marketing purposes only with your prior consent

5.3. We provide you with a clear, free and easy to implement option to withdraw your consent at any time. Please note that you have the right to opt-out of receiving direct marketing communications from us at any time by informing us of your decision via e-mail at info@nspay.lt or by using the unsubscribe link in the direct marketing communication itself.

6. Processing of personal data for statistical and / or reporting purposes

6.1. We may process the Personal Data provided by you for statistical purposes, since we, as an entity holding an electronic money institution licence, are the subject to legal requirements related to the submission of reports on the Data Controller's activities to the Bank of Lithuania.

6.2. The data concerned are processed in such a way that it would be no longer possible to identify a particular Data Subject.

7. Retention terms of Personal Data

7.1. We will store your Personal Data for as long as it is necessary for the purposes for which it was collected and processed, but no longer than required by applicable laws and regulations. After the expiry of this period, the Personal Data shall be erased/destroyed in a way that it cannot be reproduced.

7.2. If the legislation of the Republic of Lithuania does not provide for any retention period for Personal Data, this period shall be determined by us, taking into account the legitimate purpose of the retention of the data, the legal basis, and the principles of Processing of Personal Data.

7.3. The main retention terms of Personal Data:

7.3.1. in the case of the conclusion and performance of the contract, the contract shall be stored for ten (10) years after its termination;

7.3.2. we store the data of potential customers (who have been offered an offer but have not concluded the contract) for 2 (two) years from the date of the decision not to conclude the contract;

7.3.3. in order to comply with the requirements of the prevention of money laundering and terrorist financing, copies of the customer's identity documents, the beneficiary's identity data, other data obtained in the course of the identification of the customer, account and (or) contract documents shall be kept for 8 (eight) years from the date of termination of transactions or business relationship with the customer. Correspondence relating to business relationship with the customer shall be stored for a period of 5 (five) years from the date of termination of the transactions or business relationship with the customer, either in paper form or in electronic form. Retention periods may be further extended for a maximum of 2 (two) years;

7.3.4. Personal Data processed for statistical purposes usually are stored for up to 3 (three) years;

7.3.5. Payment data shall be retained for a period of 8 (eight) years from the date on which the monetary transaction was executed or the transaction was concluded. This period may be further extended for a maximum of 2 (two) years;

7.3.6. the retention period for your Personal Data processed for direct marketing purposes is 2 (two) years from the date of receipt of the relevant data, unless you withdraw such Processing of your Personal Data before the expiry of the said retention period. If this period expires or if the person withdraw the Processing of Personal Data for direct marketing purposes before the expiry of this period, we will stop processing your data.

7.4. Please note that in certain cases your Personal Data may be stored for longer:

7.4.1. if necessary to enable us to defend ourselves against claims, demands or actions and to enforce our rights;

7.4.2. we have a reasonable suspicion of illegal activity that is the subject of an investigation

7.4.3. the Personal Data is necessary for the proper resolution of a dispute or complaint;

7.4.4. on other grounds provided for by law.

8. Recipients of Personal Data

8.1. In the course of our activities, we may engage certain service providers (e.g., companies providing data storage services, companies developing and supporting software, companies providing communication services, etc.), to whom your Personal Data may be transferred. Your Personal Data is transferred to the relevant service providers only when and only to the extent necessary for the provision of their respective services.

8.2. Understanding our obligation to process your Personal Data in strict compliance with applicable requirements, we only engage service providers who have implemented/undertaken to implement appropriate technical and organizational security measures, and we ensure that these service providers comply with appropriate Personal Data protection, security and confidentiality obligations, as set out in a written agreement.

8.3. We may also provide your Personal Data to the following recipients:

8.3.1. banks and other financial institutions;

8.3.2. state institutions and registers, including the Bank of Lithuania;

8.3.3. courts, notaries, bailiffs, law enforcement authorities, etc.;

8.3.4. out-of-court dispute resolution bodies, bankruptcy administrators;

8.3.5. debt collection companies to which claims on debts are assigned;

8.3.6. service providers maintaining joint debtor data files;

8.3.7. auditors, legal and financial advisors;

8.3.8. successors to our rights and obligations;

8.3.9. the State Tax Inspectorate for the purposes of complying with tax laws, the Agreement between the Government of the Republic of Lithuania and the Government of the United States of America on Improving the Enforcement of International Tax Compliance and Implementing the Act on Enforcement of Tax Compliance Applicable to Foreign Accounts, and any other international obligations of the Republic of Lithuania in this area;

8.3.10. to other third parties in connection with the provision of our services and (or) who have a legal basis for receiving such data.

8.4. In all cases, reasonable efforts are made to ensure that Personal Data is not lost or misused in the implementation of legal requirements.

8.5. In addition, we may disclose information about you:

8.5.1. if we are required to do so by law;

8.5.2. in order to protect our rights or interests (including disclosing your Personal Data to third parties in order to collect debts owed by you to us).

8.6. We usually process Personal Data in the European Economic Area (EEA), but in some cases your personal data may be transferred outside the EEA. In such situations and when data is transferred outside the EEA, we will take all necessary measures stated by law to ensure that your personal data continues to be adequately protected. Your Personal Data may be transferred outside the EEA only under the following conditions:

8.6.1. standard contractual clauses approved by the European Commission have been signed with the data recipient, or;

8.6.2. the recipient of the data is established in a country for which the European Commission has taken an adequacy decision, i.e., the transfer of data to a data recipient in such a country will be treated as a transfer of data within the EU, or;

8.6.3. based on Article 49 of the GDPR, you gave your consent to the transfer of your Personal Data outside the EEA.

9. How we receive data from you?

9.1. We process your Personal Data that:

9.1.1. are provided to us by you;

9.1.2. are provided to us by our customers, if you are, for example, a member of their family or are a representative, employee, contractor, founder, shareholder, participant, owner, etc. of a customer - a legal entity;

9.1.3. are received by us in documents provided to us by our customers, such as account statements, payment documents, sales and other contracts, court judgments, etc.;

9.1.4. we obtain from external sources such as.:

9.1.4.1. from other financial institutions;

9.1.4.2. from supervisory and other public bodies or institutions, e.g. the Bank of Lithuania;

9.1.4.3. from the State Enterprise Centre of Registers (e.g. Population Register, Participants in Legal Persons Information System (JADIS), Beneficiaries of Legal Persons Subsystem (JANGIS), Register of Legal Persons, etc.) and other registers;

9.1.4.4. from law enforcement authorities;

9.1.4.5. from natural or legal persons (notaries, bailiffs, lawyers, etc.) when they provide Personal Data in the context of contractual or legal requirements;

9.1.4.6. from partners, suppliers or other legal persons who use us to provide services to you;

9.1.5. we receive from monitoring the use of our systems and services.

9.2. Please note that when you provide Personal Data to us, you are responsible for the accuracy, completeness and timeliness of such data. In the event that inaccurate, false or misleading Personal Data is provided, we have the right to delete such data or restrict access to services, etc. If you provide Personal Data about other persons (e.g. your relatives, employees, etc.), you are responsible for the accuracy, completeness and timeliness of such Personal Data, as well as for the consent of such person to the provision of his or her Personal Data to us. It should be noted that when you provide such data, we may ask you to confirm that you have the right to provide it. If such a person enquires from us about the receipt of his or her Personal Data, we will identify you as the provider of such data

10. Ensuring the security of Personal Data

10.1. In order to ensure the security of your Personal Data and to prevent unlawful or accidental destruction, alteration, disclosure or any other unauthorised Processing of your Personal Data, we implement different technical and organisational security measures to help us achieve these aims. These measures include various hardware and software, supplementary agreements with outsourced service providers, internal rules relating to the protection of Personal Data and other measures.

10.2. The transmission of information by electronic means of communication (e.g. email, mobile, etc.) may be less secure in individual cases for reasons beyond our control, such as chosen technical or organisational measures. Therefore, in order to ensure the security of your confidential Personal Data, we recommend that you do not provide us with information via various less secure and (or) electronic systems that we do not use.

11. Websites of third parties

11.1. We may provide links on our website to and from partners' websites, information sources, and related parties. Please note that third-party websites you access by following links on our Website have their privacy policies, and we are not responsible for them. Before submitting any of your personal data to another website, you should familiarize yourself with that website's rules, privacy policy, and other information provided on that website.

11.2. The Website contains links to our company's social networking account on LinkedIn. Please note that any information you provide to us through social networking tools (including notifications, use of the "Like" and "Follow" fields and other communications) is controlled by the controller of the social network, not us. For the reasons defined in this clause, we recommend that you familiarise yourself with LinkedIn's privacy policy.

12. Personal identification tools we use

12.1. In order to identify and verify your identity, we use the services provided by Ondato, UAB. This service provider captures a photo or video of your face and the identity document you have provided via a special website with a camera. For more information about Ondato, UAB, please refer to the Privacy Policy of this company.

12.2. The solution of Ondato, UAB is used to compare live photographs or video of your face with the identity document you have provided in order to comply with legal obligations (e.g. to comply with the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania, and other requirements for the prevention of fraud and crime), and to meet risk management obligations

12.3. The result of the facial similarity (match or non-match) will be stored for as long as it is necessary to carry out the check and for the period of time defined in the legislation on the prevention of money laundering and terrorist financing.

12.4. The facial similarity check is a one-time authorisation of a user by comparing photographs of a person against each other based on the data obtained during the check. Your facial template is not created, saved or stored. The original data cannot be retrieved from the stored information.

12.5. When using the services of Ondato, UAB, Personal Data is used to identify your identity, as Ondato, UAB compares the image of a person in a personal document with a person in a photograph. This process allows us to identify you more accurately and makes the process quicker and easier to carry out. If you are not satisfied with this method of identification, you can contact us at info@nspay.lt for another way to identify yourself

13. Rights you have as Data Subjects

13.1. As Data Subjects, you have the following rights:

13.1.1. **Access to your Personal Data and find out how they are being processed**. You have the right to receive a confirmation that your Personal Data are being processed by the Data Controller, as well as the right to access your Personal Data being processed and other related information;

13.1.2. **Request correction of incorrect, inaccurate or incomplete data**. If you believe that the information about you processed by the Data Controller is inaccurate or incorrect, you are entitled to request that this information be changed, updated or corrected;

13.1.3. **Request deletion of your Personal Data ("right to be forgotten")**. In certain circumstances specified in the legal acts (e.g. when Personal Data are being processed unlawfully, the basis for Processing the data has disappeared, etc.), you are entitled to request that the Data Controller delete your Personal Data;

13.1.4. **Request restriction of the Processing of your Personal Data**. In certain circumstances specified in the legal acts (e.g. when Personal Data is processed unlawfully, etc.), you are entitled to request that the Data Controller restrict the Processing of your data;

13.1.5. **Request to transfer of your Personal Data to another data controller or provide it directly in a form convenient for you**. In certain cases, you are entitled to transfer the data, which are processed by us with your consent and are processed by automated means, to another data controller;

13.1.6. **Disagree with the Processing of your Personal data even if they are being processed on the basis of a legitimate interest**, unless there are legitimate reasons for such Processing or they are intended to be used for bringing, enforcing legal claims or defending against them;

13.1.7. **Withdraw your consent to the Processing of your Personal Data**. In cases where your Personal Data are being processed on the basis of a separate consent, you are entitled to withdraw your consent to the Processing of your Personal Data at any time. In this case, the Data Controller will stop Processing these Personal Data of yours.

13.2. Please refer to us you queries concerning the exercise of the rights you have as Data Subjects in writing, by e-mail to info@nspay.lt.

13.3. If you believe that your Personal Data are being processed unlawfully or that your rights regarding the Processing of Personal Data are violated, please contact us by e-mail to info@nspay.lt. Your queries will be satisfied or your queries will be rejected indicating the reasons for rejection within 30 (thirty) calendar days from the date of submission of the query. The specified period of 30 (thirty) calendar days may be extended by another 60 (sixty) calendar days with prior notice, if the query concerns a large volume of personal data. The response to the query will be provided by e-mail. Upon examining your query, we will notify you of the results and the steps we have taken to fulfil your query, or provide you with information on what further actions you can take if your query has not been fulfilled or satisfied.

13.4. Your request for the exercise of rights must meet at least the following minimum requirements:

13.4.1. the request must be written, legible and understandable;

13.4.2. the request must include your name, surname and other contact details (email address, telephone number);

13.4.3. the request must contain clear and precise information about which of the above rights you wish to exercise and to what extent;

13.4.4. if the purpose of exercising the rights is to be exercised through a representative, the request must include the name and contact details of the representative and be accompanied by a document confirming the representation.

13.5. When you contact us with a verbal request to exercise your rights as a Data Subject, we shall have the right to ask you to make a written request and the obligation to specify all the possible ways in which the written request may be made and the minimum requirements applicable to the request.

13.6. You also have the right to contact the State Data Protection Inspectorate if you believe that your Personal Data is being processed in violation of your rights or legitimate interests under applicable law.

However, before contacting the State Data Protection Inspectorate, we encourage you to contact us immediately. In this way, we will be able to find together the most operative and optimal solution to the problem for both parties.

13.7. In addition, please note that the above rights of Data Subjects may be restricted in order to ensure the prevention, investigation, detection or prosecution of criminal offences or the enforcement of criminal sanctions, including the protection against and prevention of threats to public security, public safety, and in the cases of restriction of rights as set out in the Article 23 of GDPR.

14. Final provisions

14.1. We reserve the right to update the Policy and we suggest you review this Policy regularly to ensure that you are aware of any changes

14.2. By making changes, we will not reduce the scope of your rights under this Policy or applicable Personal Data protection laws. If the Policy is updated, we undertake to publish the updated version of the Policy on its Website. We also make the previous versions of the Policy available on our Website.

14.3. Amendments and (or) additions to the Policy shall become effective upon their publication on the Website.