# Privacy Policy

## Content

## I. Introduction

**UAB "INTERNATIONAL PAYMENT UNION"**, company code 304917978 (hereinafter – **the Company** or **we**), registered address at Barboros Radvilaites str. 1, LT-01124 Vilnius, Lithuania, is an electronic money institution, holding a license No. 39 issued by the Bank of Lithuania on 25 of July 2018.

As we collect and use personal data (hereinafter – **the Personal Data**), we are obligated to use and process your Personal Data only in accordance with this privacy policy (hereinafter – **the Privacy Policy**), as well as, applicable legislation, including the General Data Protection Regulation (2016/679) (hereinafter – **GDPR**), the Law on Money Laundering and Terrorist Financing Prevention of the Republic of Lithuania, Law on Legal protection of personal data of the Republic of Lithuania and other applicable legal acts.

This Privacy Policy provides basic rules for collecting, storing, processing and retention of your Personal Data and other information relating to you, as well as, the scope of processed Personal Data, the purposes, sources, recipients and other important aspects of data processing in using our services as an electronic money institution.

When writing 'you', we mean you as – a potential, existing and/or former client, our client's employee or other parties, such as beneficial owners, authorised representatives, business partners, other associated parties and/or person contacting us using e–mail or other communication measures.

Please note that in case you provide us with the information about any person other than yourself, your employees, counterparties, advisers or suppliers, you must ensure that they understand how their information will be used.

## II. Principles of processing Personal Data

The principles we follow in order to comply with the need to protect your Personal Data are as follows:

a) *principle of legality, fairness and transparency* – which means that the Personal Data with respect to you is processed in a lawful, honest and transparent way;
b) *purpose limitation principle* – which means that the Personal Data is collected for specified, clearly defined and legitimate purposes and shall not be further processed in a way that is incompatible with those purposes;
c) *data reduction principle* – which means that the Personal Data must be adequate, appropriate and is only necessary for the purposes for which it is processed;
d) *accuracy principle* – which means that the Personal Data must be accurate and, if necessary, updated. All reasonable steps must be taken to ensure that Personal Data which is not accurate in relation to the purposes for which it is processed shall be immediately erased or corrected;

e) *the principle of limitation of the length of the storage* – which means that the Personal Data shall be kept in such a way that your identity can be determined for no longer than is necessary for the purposes for which the Personal Data is processed;
f) *integrity and confidentiality principle* – which means that the Personal Data shall be managed by applying appropriate technical or organizational measures in a way, which would ensure the proper security of the Personal Data, including the protection from an unauthorized processing or processing of an unauthorized data against accidental loss, destruction or damage.

Your Personal Data is considered as confidential information and may only be disclosed to third parties in accordance with the rules and procedure provided in this Privacy Policy and the applicable legal acts.

## III. Categories of Personal Data being processed

The Personal Data we collect can be grouped into the following categories:

| Type of information | Personal data |
|---|---|
| Basic Personal Data | name, surname, job title etc. |
| Identification information and other background verification data *(your or your representative's, ultimate beneficiary owner's of legal entities)* | name, surname, personal identity code, date of birth, address, nationality, gender, passport or ID card copy, evidence of beneficial ownership or the source of funds, number of shares held, voting rights or share capital part, title, visually scanned or photographed image of your face or image that you provide through a mobile application or camera, video and audio recordings for identification, telephone conversations to comply with client due diligence/"know your client"/anti-money laundering laws and collected as part of our client acceptance and ongoing monitoring procedures. |
| Financial data | transactional data (e.g. beneficiary details, date, time, amount and currency which was used, name/IP address of sender and receiver), accounts, amount of transactions, income, location, etc. |
| Information related to legal requirements | data resulting from enquiries made by the authorities, data that enables us to perform anti-money laundering requirements and ensure the compliance with international sanctions, including the purpose of the business relationship and whether you are a politically exposed person and other data that is required to be processed by us in order to comply with the legal obligation to "know your client". |

| | |
|---|---|
| Contact Data | registered/actual place of residence, phone number, e–mail address etc. |
| Any other Personal Data related to you that you may provide | |

## IV. Purposes and legal basis for Personal Data processing

| Purpose | Legal basis | Categories of Personal Data |
|---|---|---|
| Conclusion of the contract or for performance of measures at your request prior to the conclusion of the contract (to get to know, identify and verify our clients) | 1. to take the necessary steps before the conclusion of the contract;<br>2. legitimate interests;<br>3. complying with regulations applicable to us. | Basic Personal Data;<br>Identification and other background verification data;<br>Contact Data;<br>Other Personal Data needed (in order to identify the possibility of providing services). |
| For the fulfilment of a contract concluded with you, including but not limited to provision of services of issuance, distribution and redemption of electronic money and provision of payment services | 1. contract performance;<br>2. legitimate interests;<br>3. complying with regulations applicable to us; | Basic Personal Data;<br>Identification and other background verification data;<br>Financial data;<br>Information related to legal requirements;<br>Contact Data;<br>Other Personal Data provided to us by or on behalf of you or generated by us in the course of providing services. |
| To comply with legal obligations (e.g. implementation of the obligations under the Law on Money Laundering and Terrorist Financing Prevention of the Republic of Lithuania and other fraud and crime prevention purposes) and risk management obligations) | 1. complying with regulations applicable to us;<br>2. legitimate interests. | Basic Personal Data;<br>Identification and other background verification data;<br>Financial data;<br>Information related to legal requirements;<br>Contact Data;<br>Other Personal Data provided to us by or on behalf of you or generated by us in the |

| | | |
|---|---|---|
| | | course of providing our services. |
| To provide an answer when you contact us through our website or other communication measures | 1. your consent;<br>2. legitimate interests. | Basic Personal Data;<br>Contact Data;<br>Other Personal Data provided to us by you. |

What do we mean when we say:

*Legitimate Interest*: the interest of ours as a business in conducting and managing our services to enable us to provide to you and offer the most secure experience.

*Contract performance*: processing your Personal Data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

*Legal Obligation*: processing your Personal Data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

## V. Direct marketing

We may use our existing clients’ e–mail for our similar goods or services marketing. In case you do not object to the use of your e-mail for the marketing of our similar goods and services and you are granted with clear, free of charge and easily realisable possibility to object or withdraw from such use of your contact details by sending each message.

We may also provide the information to you being our client about our products or services by sending the messages in the application and such messages may be viewed in the notification center, in case you do not choose the “opt-out” function in our application.

In other cases, we may use your Personal Data for the purpose of direct marketing, if you give us your prior consent regarding such use of data.

We are entitled to offer the services provided by our business partners or other third parties to you or find out your opinion on different issues in relation to our business partners or other third parties on the legal basis for this, i.e. on the basis of a prior consent.

In case you do not agree to receive these marketing messages and/or calls offered by us, our business partners or third parties, this will not have any impact on the provision of services to you as the client.

We provide a clear, free-of-charge and easily realisable possibility for you at any time not to give your consent or to withdraw your given consent for sending proposals put forward by us. We shall state in each notification sent by e-mail that you are entitled to object to the processing of the Personal Data or refuse to receive notifications from us. You shall be entitled to refuse to receive notifications from us by clicking on the respective link in each e-mail notification.

## VI. How do we obtain your Personal Data?

We collect information you provide directly to us. For example, when becoming a new client (if you have entered into or seek to enter into an agreement with us). The Company also collects information which you provide us with such as messages that you have sent us (e.g. completing a form on our website or mobile application, registration for our services), by access and use of our website or mobile application, by setting up an account with us, when you subscribe to our electronic publications (e.g. newsletters).

Personal Data that we may collect from third parties:

a) when it is provided to us by a third party which is connected to you and/or is dealing with us, for example, business partners, sub–contractors, service providers, merchant and etc.;
b) third party sources, for example, register held by governmental agencies or where we collect information about you to assist with “know your client” check-ups as part of our client acceptance procedures such as sanctions list, politically exposed persons list and etc.;
c) from banks and/or other finance institutions in case the Personal Data is received while executing payment operations;
d) from publicly available sources – we may, for example, use sources to help us keep your contact details that we already possess accurate and up to date or for professional networking purposes or for providing our services;
e) from other entities in the Company Group or other entities which we collaborate with.

## VII. Who do we share your Personal Data with?

We may transfer your Personal Data in accordance with the principles of confidentiality to the following categories of recipients:

a) our business partners, agents or intermediaries who are a necessary part of the provision of our products and services, as well as, card organizations (such as VISA or MasterCard) – in connection with our payment services;
b) governmental bodies and/or supervisory authorities (in accordance with the requirements and obligations under the provisions of legal acts concerning anti-money laundering, fraud prevention, counter terrorist financing), credit, financial, payment and/or other electronic money institutions;
c) pre-trial investigation institutions, the State Tax Inspectorate;
d) lawyers, bailiffs, auditors etc.;
e) service providers, who make your identity verification by using their IT solutions;
f) companies providing services for money laundering, politically exposed persons and terrorist financing check-up and other fraud and crime prevention purposes and/ or companies providing similar services;
g) external service providers (that provide such services as, for example, system development and/or improvement, audit services);
h) beneficiaries of transaction funds receiving the information in payment statements together with the funds of the transaction;
i) when the Services are provided using the CENTROlink payment system of the Bank of Lithuania, the personal data provided in the payment order and the transfer order shall be processed in the

CENTROlink system in accordance with the Resolution of the Board of the Bank of Lithuania No. 03-204 "On Approval of the Rules of Concluding the Contract for the Holder of the Addressable BIC in the Payment System of the Bank of Lithuania CENTROlink", dated 22 December 2015 (TAR, TAR, 23-12-2015, No. 2015-20365; 10-11-2017, No. 2017-17680).

j) other entities that have a legitimate interest or the Personal Data may be shared with them under the contract which is concluded between you and us;
k) other entities under an agreement with us.

## VIII. International transfer of Personal Data

As we provide international services your Personal Data may be transferred and processed outside the European Union (hereinafter – **the EU**) and the European Economic Area (hereinafter – **the EEA**).

The transfer of Personal Data may be considered as needed in such situations as, e.g.:

a. in order to conclude the contract between you and us and/or to fulfill the obligations under such contract;
b. in cases indicated in laws and regulations for protection of our lawful interests, e.g. in order to bring proceedings in court/other governmental bodies;
c. in order to fulfill legal requirements or in order to realize public interest.

In case your Personal Data is transferred outside the EU and the EEA, we will take all steps to ensure that your data is treated securely and in accordance with this Privacy Policy and we will ensure that it is protected and transferred in a manner consistent with the legal requirements applicable to the Personal Data.

This can be done in a number of different ways, for example:

a) the country to which we send the Personal Data, a territory or one or more specified sectors within that third country, or the international organization is approved by the European Commission as having an adequate level of protection;
b) the recipient has signed standard data protection clauses which are approved by the European Commission;
c) if the recipient is located in the US, it may be a certified member of the EU–US Privacy Shield scheme;
d) special permission has been obtained from a supervisory authority.

We may transfer Personal Data to a third country by taking other measures if it ensures appropriate safeguards as indicated in the GDPR.

## IX. Automated decision-making

In some cases, we may use automated decision-making which refers to a decision taken solely on the basis of automated processing of your Personal Data.

Automated decision-making refers to the processing using, for example, a software code or an algorithm, which does not require human intervention.

We may use forms of automated decision making on processing your Personal Data for some services and products. You can request a manual review of the accuracy of an automated decision in case you are not satisfied with it.

## X. How do we protect your Personal Data?

We ensure the implementation of appropriate technical and organizational and administrative security measures required to ensure the security of your Personal Data processing, in order to protect your Personal Data from loss, misuse, accidental or unlawful destruction, modification, disclosure, unauthorized access or any other unlawful handling.

The Company and any third-party service providers that may engage in the processing of Personal Data on our behalf (for the purposes indicated above) are also contractually obligated to respect the confidentiality of the Personal Data.

## XI. Retention terms of Personal Data processing

We will keep your Personal Data for as long as it is needed for the purposes for which your data was collected and processed but no longer than it is required by the applicable laws and regulations. This means that we store your data for as long as it is necessary for providing services and as required by retention requirements in laws and regulations. If the legislation of the Republic of Lithuania does not provide any period of retention of Personal Data, this period shall be determined by us, taking into account the legitimate purpose of the data retention, the legal basis and the principles of lawful processing of Personal Data.

The terms of data retention of the Personal Data for the purposes of the processing of the Personal Data as specified in this Privacy Policy are as follows:

a) as long as your consent remains in force, if there are no other legal requirements which shall be fulfilled with regard to the Personal Data processing;
b) in case of the conclusion and execution of contracts – until the contract concluded between you and the Company remains in force and up to 10 years after the relationship between the client and the Company has ended;
c) the Personal Data collected for the implementation of the obligations under the Law on Money Laundering and Terrorist Financing Prevention shall be stored in accordance with the Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania up to 8 (eight) years. The retention period may be extended for a period not exceeding 2 (two) years, provided there is a reasoned request from a competent authority;
d) the Personal Data submitted by you through our website is kept for an extent necessary for the fulfilment of your request and to maintain further cooperation, but no longer than 6 months after the last day of the communication, if there are no legal requirements to keep them longer.

In the cases when the terms of data keeping are indicated in the legislative regulations, the legislative regulations are applied.

Your Personal Data might be stored longer if:

a) it is necessary in order for us to defend ourselves against claims, demands or action and exercise our rights;
b) there is a reasonable suspicion of an unlawful act that is being investigated;
c) your Personal Data is necessary for the proper resolution of a dispute/ complaint;
d) under other statutory grounds.

## XII. What rights do you have in relation to your Personal Data?

You as a data subject have rights in respect of Personal Data, we hold on you. Under certain circumstances and in accordance with EU or other applicable data protection laws, you may have the right to:

a) **get familiar with your Personal Data and how it is processed** – you have the right to obtain information about which Personal Data about you that we process. Your right to access may, however, be restricted by legislation, protection of other persons' privacy and consideration for the Company's business concept and business practices. The Company's know-how, business secrets as well as internal assessments and material may restrict your right of access;
b) **demand rectifying incorrect or incomplete data** – if it turns out that we process Personal Data about you that is inaccurate, you have the right to request a rectification of the Personal Data. You can also request to have incomplete Personal Data about you completed;
c) **erasing your Personal Data** – you have the right to have any or all of your Personal Data erased. In certain cases, we cannot erase all of your Personal Data. In such case this would be due to the fact that we need to store your Personal Data due to a contractual relationship or law;
d) **restricting the processing of your Personal Data** – you have the right to demand that our processing of your Personal Data be restricted for a period of time. This can pertain, for example, to a situation where you believe data about you is inaccurate and we need to verify it. It can also pertain to a situation where you object to processing that we base on a legitimate interest. In such case we must verify if our grounds override yours;
e) **transfer your Personal Data** to another data controller or provide directly to you in a convenient format (NOTE: applicable to Personal Data which is provided by you and which is processed by automated means on the basis of consent or on the basis of conclusion and performance of the contract);
f) **object to any processing based on the legitimate interests** ground unless our reasons for undertaking that processing outweigh any prejudice to your data protection rights;

g) **to withdraw your consent** so that we stop that particular processing, when the processing is based on consent. However, such consent withdrawal does not affect the lawfulness of processing based on consent before its withdrawal;
h) **not to be subject to a decision based solely on automated processing**;
i) **lodge an appeal to the State Data Protection Inspectorate –** if you have an objection about how we have processed your Personal Data, you can turn to the supervisory authority concerned.

We will exercise your rights only after we receive your written request to exercise a particular right indicated above and only after confirming the validity of your identity. The written request shall be submitted to us by personally appearing at the registered office address of the Company, by ordinary mail or by e-mail: support@interpaylink.com.

Your requests shall be fulfilled or fulfilment of your requests shall be refused by specifying the reasons for such refusal within 30 (thirty) calendar days from the date of submission of the request meeting our internal rules and GDPR. The afore-mentioned time frame may be extended for 30 (thirty) calendar days by giving a prior notice to you if the request is related to a great scope of Personal Data or other simultaneously examined requests. A response to you will be provided in a form of your choosing as the requester.

## XIII. The right to lodge a complaint

You can file a complaint regarding the Personal Data in the same manner as specified above the section XII.

You can also address the State Data Protection Inspectorate with a claim regarding the processing of your Personal Data if you believe that the Personal Data is processed in a way that violates your rights and legitimate interests stipulated by applicable legislation. You may apply in accordance with the procedures for handling complaints that are established by the State Data Protection Inspectorate and which may be found by this link: https://www.ada.lt/go.php/Skundu-nagrinejimas378.

## XIV. How changes to this Privacy Policy will be made?

We regularly review this Privacy Policy and reserve the right to modify it at any time in accordance with applicable laws and regulations. Any changes and clarifications will take effect immediately upon their publication on our website: www.interpaylink.com.

Please review this Privacy Policy from time to time to stay updated on any changes.

## XV. Cookies Policy

If you access our information or services through our website, you should be aware that we use Cookies.

For more information on how to control your Cookie settings and browser settings or how to delete Cookies on your hard drive, please read the Cookies Policy available on our website: www.interpaylink.com .

## XVI. Contact us

You can contact us by writing to us at support@interpaylink.com or post us at UAB “International Payment Union” – Barboros Radvilaites str. 1, LT-01124 Vilnius, Lithuania.

You can also contact our Data Protection Officer by sending an e-mail to the address: privacy@interpaylink.com.