NIUM

PRIVACY NOTICE

FEBRUARY 2020
LITHUANIA

1. PRIVACY NOTICE

UAB „NIUM EU" (formerly known as UAB "InstaReM EU", hereinafter "InstaReM (powered by NIUM)", "we", "us"), code 304548794, having the license issued by the Bank of Lithuania No. 14 on 28th September 2017, respects your rights to privacy. InstaReM (powered by NIUM) deals with personal information collected in accordance with this Privacy Notice (hereinafter - Notice) when you visit or use our website or mobile application in the European Economic Area. When used in this Notice, „personal information" refers to any information or opinion, which relates directly or indirectly to you. This includes any information that can be used to distinguish, identify or contact you.

Our Notice is to comply and ensure that our employees comply with the requirements of any applicable laws and legal acts of the Personal Data protection on the level of country where we operate as well as with applicable legal acts of the European Union. InstaReM (powered by NIUM) will commit itself, on its own initiative, to follow the good practice principles provided by the Bank of Lithuania.

Please read the following carefully to understand our practices regarding Personal Data and how InstaReM (powered by NIUM) will process it.

2. DATA SUBJECT AND COLLECTING OF DATA

We can collect personal data directly from the following persons:

a) potential, existing and former clients of InstaReM (powered by NIUM), business, partners, agents, outsources, intermediaries, employees, potential employees;

b) persons (e.g. representatives, proxies, beneficiary owners, family members, spouses, partners, heirs, guarantors, etc.) connected with the aforementioned persons;

c) any person contacting InstaReM (powered by NIUM) using e-mail, phone and other available communication means, both online and offline.

3. WHY DO WE COLLECT YOUR PERSONAL INFORMATION?

We use your information in the following ways:

a) provision of payment services and issuance, distribution and redemption of electronic money;

b) to carry out our obligations relating to your contracts with us;

c) to conduct your identification;

d) to verify your identity to protect against fraud, to comply with our legal obligations (performing client due diligence/"know your client", anti-money laundering and counter terrorist financing, sanctions or reputational risk screening, identifying conflicts of interests);

e) to provide you with the information, products and services that you request from us;

f) to comply with any applicable legal and/or regulatory requirements;

g) to notify you about changes in our Services;

h) to provide you with better customer services and products;

i) to administer our Services and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;

j) to provide you with information about other similar goods and services we offer, if we have your consent for this;

k) to provide you, or permit selected third parties to provide you, with information about goods or services we feel may interest you, if we have your consent for this;

l) to process your job application.

4. WHO GIVES US THE RIGHT TO RECEIVE AND USE YOUR PERSONAL DATA?

The legal grounds, in accordance with which we process personal data are follows:

a) processing is necessary for fulfilment of a contract concluded with you or on behalf of you or for performance of measures at the request of your prior to the conclusion of the contract;

b) processing is necessary in order to fulfil a legal or regulatory duty applicable to the InstaReM (powered by NIUM);

c) your consent to the processing of the personal data for one or more specific purposes;

d) processing is necessary for protection and fulfilment of the InstaReM (powered by NIUM) legitimate interest.

InstaReM (powered by NIUM) legitimate interest are follows:

a) to carry out commercial activities;

b) offering InstaReM (powered by NIUM) services;

c) improving InstaReM (powered by NIUM) services, as well the quality of services;

d) ensuring the fulfilment of contractual obligations, including consideration of the claims and complains;

e) keep transactions history for accounting, reporting and analytics purposes;

f) addressing public bodies, law enforcement bodies and courts to protect its legal interests.

5. HOW DO WE COLLECT PERSONAL INFORMATION?

Most of the personal information is collected directly from you by the following means:

a) through the access and use of the InstaReM (powered by NIUM) website or mobile application;

b) through your registration for our Services and/or by setting up an account with us;

c) through your response to our loyalty program, a contest or claim to a prize announced by us from any financial transaction you make with InstaReM (powered by NIUM);

d) through your subscription to our electronic publication such as newsletters, rate broadcast;

e) from 3rd party connected with you and/or dealing with us;

f) from the commercial banks and finance institutions (the data are received during the execution of payment operations);

g) directly through your job application on our site or from 3rd party sites or recruitment consultants with whom we have an agreement;

h) from InstaReM employees when they are referring us to you;

i) from remitters.

6. WHAT KIND OF PERSONAL INFORMATION DO WE COLLECT AND RESERVE?

The types of personal information that we collect, and share depend on the product or service you avail with us. It includes, but is not limited to:

a) contact and personal information: title, your first name, surname, date of birth, email address, mobile phone number, personal code, residential address and/or mailing address, data of the personal identity document, photo, signature, employment status, source of funds, driving license number, sex, citizenship;

b) account information: financial institution account number, IBAN, debit card number. Account information: account details and transaction history, date of the transaction, amount, currency, location, data about beneficiary (natural person's name, date of birth, personal identification number or other unique character sequence assigned to this person for identifying the person; the legal entity's name, legal form, registered office, code if any) and other details about the parties involved;

c) other information: video and audio records of video calls for identification, telephone conversations, IP address;

d) special categories of personal data: political opinions (politically exposed person), biometric data as described in section 6 a, c, i;

e) details of client visits to website, app and the resources that client's access;

f) for the purpose of direct marketing: name, surname, telephone no., e-mail address, address, date of birth, location, IP address, country of residence, nationality, industry type, employment status, cookies;

g) for the purpose of recruitment: name, surname, nationality, address, employment/visa status, telephone no., e-mail address, education, work experience, current and previous employers contacts with candidates' consent;

h) for statistical, analytical and our services improvement purposes, we can use anonymized and aggregated datasets, which can be used not limited to modeling, reporting and analytics;

i) data collected about legal entities:

I. representatives of legal entities (members of the management bodies and other representatives (for example, employees) who are authorized to represent the client in relations with the controller or acting on their behalf, representing the client on behalf of the client, according to corporate documents): personal identification number, identity document details, workplace, e-mail address, gender, position, surname, nationality, telephone number, name, photo, signature, bank account information (bank name and bank account number), monetary transaction or transaction date, amount, currency, the data on the beneficiary of the funds (natural person's name, date of birth, personal identification number or other unique character sequence assigned to this person for identifying the person; the legal entity's name, legal form, registered office, code if any);

II. beneficiaries of legal entities (natural persons who directly or indirectly own or control a legal entity, having a sufficient number of shares or voting rights, including through bearer share management): personal identification code, identity document, gender, surname, nationality, name, photo, signature, the number of shares held, the voting rights or the share capital held, the date of the monetary transaction or transaction, the amount in the currency in which the monetary transaction or transaction is carried out, the data on the beneficiary (natural person's name, surname, date of birth , personal code or other unique character assigned to this person to identify the person; the legal entity's name, legal form, home address, code, if any).

7. WHO DO WE DISCLOSE YOUR PERSONAL INFORMATION TO, AND WHY?

We may share your personal information with other companies in the InstaReM (powered by NIUM) Group as well as with users of payments services (payees and payers) and financial institutions, the Bank of Lithuania and participants of SEPA (due to the using of Single Euro Payments Area -SEPA). Sometimes we may disclose your personal information to organizations outside the InstaReM (powered by NIUM) Group such as:

a) to our contractors or service providers for the purposes of conducting business and providing our services or products to you, including web hosting providers, IT systems administrators and payment processors;

b) to companies providing services for money laundering, politically exposed persons and terrorist financing check-up and other fraud and crime prevention purposes and companies providing similar services, including regulatory bodies with whom such personal data is shared;

c) to companies providing service for validation and verification the identity and location of our customers;

d) to our intermediary banks in order to process certain transactions on your behalf, for example, by disclosing your name and address;

e) to any of our partners, agents or intermediaries who are a necessary part of the provision of our products and services;

f) to international intermediaries to complete your transactions;

g) to any government regulatory bodies that normally require it or may request it.

The below mentioned are our main partners, including, but not limited to, those we will share your information and who are acting on behalf of us:

a) **Onfido** - InstaReM (powered by NIUM) makes your identity verification using Onfido solution for such identification and verification. Onfido solution are used to scan or make photo image of your face or image that your provide through a mobile app or camera, video and audio record for identification, as well comparing live photograph data or video record of yourself and your ID document, to comply with client due diligence/"know your client"/anti-money laundering laws and collected as part of our customer acceptance and ongoing monitoring procedures. Result of the identity verification and related data will be retained how long it is necessary to carry out identity verification and for the period required by laws on Anti-Money laundering. Please read more about Onfido solution for identity verification here https://onfido.com/. If you do not feel comfortable with this identification method you may contact us by email support@InstaReM.com for alternative way to identify yourself.

b) **GB Group Plc** - InstaReM (powered by NIUM) is performing client due diligence/ „know your client" using GB Group Plc solution. GB Group Plc solution helps us validate address elements within your submitted records. We provide your name, surname, date of birth and address and GB Group Plc check it in databases. Please read more about GB Group Plc solution here https://www.gbgplc.com.

We ensure that taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, we implement appropriate technical and organizational measures to protect your Personal Data. We ensure that the same requirements on the technical and organizational measures are applied by the parties to whom we may transfer your data.

8. SECURITY OF INFORMATION COLLECTED

To help protect your personal information from unauthorized access and use, we endeavor to use reasonable security measures. These measures can include physical, electronic and procedural safeguards such as computer safeguards and secured files and buildings. We also endeavor to limit access to personal information to only employees, agents and representatives that need to know.

Always use caution and good judgment when sending money and when using the internet and mobile technologies. Please be aware, that third parties may unlawfully intercept or access your personal information, transmissions to us, or may wrongly instruct you to disclose information to them by posing as InstaReM or by misinforming you about our Services. Do not disclose your passwords, full card and account numbers or your full personal number by phone or e-mail. If you have noticed a security violation or bug in respect to our services or have received a suspicious message, please do not hesitate to write us at Support@InstaReM.com.

9. DO WE DISCLOSE PERSONAL INFORMATION OVERSEAS?

We may disclose your personal information to recipients located outside the European Economic Area (hereinafter – the EEA). These entities may include:

a) InstaReM (powered by NIUM) Group companies;

b) InstaReM (powered by NIUM) Group service providers;

c) International Intermediaries.

To effect, administer and complete transactions or deliver products or services including, but not limited to:

a) companies which help us run or improve the running of our business or which help us deliver products and services to you and to banks, card companies, reference agencies, etc.

b) in order to comply with legal, regulatory, security and processing requirements, government (domestic and international) requirements, applicable to us or our affiliates or service providers, including but not limited to anti-money laundering laws; and

c) to organizations which help us process transactions, validate customer information, and prevent debt, fraud, theft or loss.

Where we transfer your personal information outside EEA, we will ensure that it is protected and transferred in a manner consistent with legal requirements applicable to the information. This can be done in a number of different ways, for instance:

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 a satisfactory 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 and is a certified member of the EU–US Privacy Shield scheme;

d) in case a special permission has been obtained from a supervisory authority;

e) in other circumstances, the law may permit us to otherwise transfer your personal information outside Europe;

f) in all cases, however, any transfer of your personal information will be compliant with applicable data protection law.

10. DO WE USE OR DISCLOSE PERSONAL INFORMATION FOR MARKETING?

We will use your personal information to offer you products and services that we believe may interest you only if we have your consent for this kind of offering. We will not do if you withdraw your consent.

Please be informed that you shall have the right to refuse from the processing of your Personal Data for the purpose of direct marketing by the same method as you consented with the processing of personal data for direct marketing. The services can be unsubscribed by updating your profile page on InstaReM (powered by NIUM) website or by clicking on the „unsubscribe link" in each e-mail notification.

We may disclose information about current and former customers to perform marketing, business analysis and advertising services to companies with whom we have contractual or joint marketing arrangements upon notice that you have provided unambiguous consent (opt-in) for the use of Information for these purposes.

We also have relationships with advertising companies, who may use cookies, pixels, web beacons, app or device information or related information to display advertising tailored to your interests or location. To opt-out of tailored advertising delivered by other advertising companies, you should choose the appropriate settings in your browser(s)

(e.g., block cookies), device (e.g., turn “Location” off) and app(s). Please note that if you do not accept cookies or change your device or app settings, you may experience some inconvenience in your use of our website or app and some online or mobile products and services.

11. RETENTION OF YOUR PERSONAL DATA

The length of time we retain your personal data is determined by a number of factors including the purpose for which we use that information and our obligations under other laws. It means that 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.

We will store your personal 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 defined in this Notice are following:

a) we retain your personal data as long as your consent remains in force, if there are no other legal requirements which shall be fulfilled concerning Personal Data’s processing;

b) in case of the conclusion and execution of contracts – we retain your personal data until the contract concluded between you and us remains in force and up to 10 years after the contractual relationship between you and us has ended;

c) your personal data which has been collected in order to fulfill the obligations under the Law on Money Laundering and Terrorist Financing Prevention in a proper way shall be stored in accordance with the provisions of Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania, mainly – up to 8 (eight) years. The afore-mentioned period may be extended for a period not exceeding 2 (two) years, provided there is a reasoned request from a competent authority;

d) your personal data which has been submitted by you during the started but not completed registration is stored for a period which is necessary for the fulfilment of registration and offer new products, but no longer than 3 years after the start of registration, in case there are no legal requirements to keep them longer;

e) your personal data which has been submitted by you through our website is kept for a period which is necessary for the fulfilment of your request and to maintain further cooperation, but no longer than 3 years after the last day of the communication, in case there are no legal requirements to keep them longer;

f) your personal data which has been submitted by you for recruitment purpose will be deleted after the end of the screening.

Please also be informed that under some circumstances, your personal data might be stored longer, mainly:

a) in case it is necessary in order for us to defend ourselves against claims, demands or action and in order to exercise our rights in a proper way;

b) in case there is a reasonable suspicion of an unlawful act that is being investigated;

c) in case your personal data is necessary for the proper resolution of a dispute/ complaint;

d) under other statutory grounds.

12. RIGHTS IN RELATION TO PERSONAL DATA PROCESSING

You as a data subject have a number of rights in relation to your personal data. Under certain circumstances and in accordance with applicable data protection laws, you may have these rights:

a) right to be informed about the processing of your personal data;

b) right to rectification of incorrect or incomplete data, right to erasure your personal Data or right to restriction of processing of your personal data when personal data is processed without complying with legal requirements or when there is another legal basis;

c) right to transfer your personal data to another data controller or provide directly to you in a convenient format (NOTE: applicable to the 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);

d) right to 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;

e) right to withdraw your consent so that we stop that particular processing, when the processing is based on consent;

f) right to lodge a complaint to the State Data Protection Inspectorate.

In this respect, you may receive a copy of the Personal Data that we hold on file. For any further copies, we reserve the right to charge a reasonable fee based on administrative costs. To exercise this right, please contact us as indicated in this Notice. All other rights of data subject are granted to you according to the applicable law and in compliance with our internal rules of personal data protection.

We retain your personal data for the period necessary to carry out the purposes outlined in this Notice, unless a longer period is required or permitted by law.

13. AUTOMATED DECISION MAKING

Automated Decision Making refers to a decision which is taken solely on the basis of automated processing of your personal data. This means processing using, for example, 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. Where we engage in automatic decision-making, we implement suitable measures to safeguard your rights and freedoms and legitimate interests, at least the right to obtain human intervention from us in the course decision-making process.

Automated decision making is legitimate to use, because it is needed for entering into a contract between you and us.

We have a legitimate interest to use profiling for example when conducting analysis for marketing purposes or monitoring transactions in order to detect frauds.

14. RESOLVING YOUR PRIVACY CONCERNS AND COMPLAINTS - YOUR RIGHTS

We exercise your rights only after receiving your written request to exercise a particular right and only after confirming the validity of your identity.

After identifying yourself and signing the written request to exercise your rights, the request shall be submitted to us by personally appearing at by ordinary mail or by e-mail: privacy@InstaReM.com.

If submitted by e-mail, the format and content of the request must be in an electronic format recognized, opened and processed by electronic document management systems or other information technology tools used by us.

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. The afore-mentioned time limit may be extended for 30 (thirty) calendar days by giving a prior notice to you if the request is related to great scope of personal data, other simultaneously examined requests.

If you have a reasonable doubt or a suspicion that your personal data processing is taking place in contradiction to the requirements laid in the General data Protection regulation, you may submit a complaint on violence of Personal data Processing to the State Data Protection Inspectorate as well to apply to the competent court. 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.

Where permitted by law, we reserve the right to collect a service charge for providing you any information in connection with your request.

15. COOKIES NOTICE

To ensure our website works correctly, we may at times place a small piece of data known as a cookie on your computer or mobile device.

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 Notice which is available on our website: https://www.InstaReM.com/Notice/EU-cookie-Notice.pdf

16. CHANGES IN THE PRIVACY NOTICE

InstaReM (powered by NIUM) reserves the right to modify this Notice, however, your privacy will not be reduced without your consent. We urge you to review this Notice when you visit to obtain the most current version.

17. CONTACT US

You can contact us by writing to us at support@InstaReM.com or post us at UAB „InstaReM (powered by NIUM) EU“, code 304548794, registered address at Konstitucijos pr. 21 B, Vilnius, the Republic of Lithuania.

Our Privacy Officer can also be contacted in relation to privacy concerns by writing to privacy@InstaReM.com.

NIUM