Privacy Policy

Okeo Payments UAB

Last update: 10 February 2021

Purpose and scope

"**Okeo Payments, UAB**" (also referred to as **we**, **us**, **Okeo Payments**, **Company**) is an electronic money institution licensed by the Bank of Lithuania (license no. 71), incorporated and existing in Vilnius, Lithuania, company registration number 305219549, having its registered office at Gedimino pr. 20, LT-01103, Vilnius.

Okeo Payments is committed to protect the privacy of your personal data in accordance with the applicable laws, 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 referred to in this Policy as the data protection law. We value your privacy and we only collect and use your personal data in accordance with this Policy and binding provisions of the law.

In this Privacy Policy we provide you with explanation on what kind of personal data we collect when providing you with our services of issuance, distribution and redemption of electronic money and payment services (further jointly referred to as "Services"). We render the Services via our web-based platform, our web page at www.okeo.com, our developer portal (for Open Banking) at https://developer.okeo.com/ and through communication channels for some ancillary services (e.g. email and telephone while providing the Client support). In addition, in this Policy we describe how we use your personal data, who we share it with, how we protect it and other important aspects of data processing when using our Services.

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

Please read carefully the following Policy and if you have any questions regarding processing of your data you can contact our Data Protection Officer at dpo@okeo.com. We keep this Policy under regular review and publish updates on our web page www.okeo.com. Please review this Privacy Policy from time to time to stay up to date with the changes.

Personal Data Controller

Under the data protection law, Okeo Payments is the Data Controller responsible for handling your personal data processed in relation to the Services. In this context the term "personal data" means any

information which can be used to personally identify you (e.g. a combination of your name and postal address).

As a Personal Data Controller, we are responsible for ensuring security of your personal data made available to us, in particular to prevent unauthorized access to your data. We are also responsible for ensuring all users with the opportunity to benefit their rights regarding their own personal data, like the right to access or erase. When processing personal data, we follow the principles of a) legality, fairness and transparency; b) purpose limitation; c) data reduction; d) accuracy; e) limitation of the length of the storage; f) integrity and confidentiality.

What information we collect, for what purposes and on what legal basis

Categories of personal data being processed

The personal data we collect can be grouped into the following categories:

Type of information	Personal data
1. Basic personal data	First, last, middle, maiden names, job title, etc.
2. Identification information and other background verification data (your, or your representatives' and, ultimate beneficiary owner's)	Name, surname, personal identity code, date of birth, country of birth, address, nationality, citizenship, gender, passport or ID card copy and its details (e.g. type, number, issuance place and date, expiry date, MRZ code, signature), evidence of beneficial ownership or the source of funds (funds for account opening or transactions, occupation/employment information), source of wealth (information on how wealth was obtained), tax information (tax residence, tax identification number), 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 or desktop camera while using our identification application, video and audio recordings for identification, telephone conversations
3. Monetary operations details	Such as currency, amount, location, date, time, currency, your IP address, payer's and payee's name and registration information, messages and documents sent or received with the payment
4. Details of your activities in our web-based platform and developer portal	History of the actions performed with reference to your payment account when using the Services (e.g. inviting new user, changing permissions of existing users, changing own authorisation limits), technical information, including the internet protocol (IP) address used to connect your computer to the internet, your log-in information (e.g. login time), the browser type and version, the time-zone setting, the operating system and platform, the type of device you use, a unique device identifier (for example, the MAC address of the device's wireless network interface)
5. Details of your existing bank account/-s	Financial institution account number, IBAN number, payment card number

Type of information	Personal data
6. 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"
7. Contact details	Phone number, email
8. Special category data	Biometrical data

Purposes and legal basis for personal data processing

Purpose	Legal basis	Categories of personal data
1. For the conclusion of the contract or for performance of measures at your request prior the conclusion of the contract.	• Taking necessary steps before the conclusion of the contract; • Legal obligations.	• Basic personal data; • Identification and other background verification data; • Contact details; • Other personal data needed (in order to evaluate the possibility of providing services).
2. For the fulfilment of the contract concluded with you, including but not limited to the provision of the Services.	• Contract performance; • Legal obligations.	• Basic personal data; • Identification and other background verification data; • Monetary operation details; • Details of your activities in our web-based platform and developer portal; • Details of your existing bank account/-s; • Information related to legal requirements; • Contact details; • Other personal data needed (in order to evaluate the possibility of providing services).
3. 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	• Legal obligations.	• Basic personal data; • Identification and other background verification data; • Monetary operation details; • Details of your activities in our web-based platform and developer portal; • Details of your existing bank account/-s;

Purpose	Legal basis	Categories of personal data
purposes) and risk management obligations		• Information related to legal requirements; • Contact details; • Other personal data needed (in order to evaluate the possibility of providing services).
4. For remote identification of your personal identity	• Your consent.	• Identification and other background verification data; • Special category data.
5. To prevent, limit and investigate any misuse or unlawful use or disturbance of the Services or to establish, exercising and defend legal claims	• Contract performance; • Legitimate interest; • Legal obligations.	• Basic personal data; • Identification and other background verification data; • Monetary operation details; • Details of your activities in our web-based platform and developer portal; • Details of your existing bank account/-s; • Information related to legal requirements; • Contact details; • Other personal data needed (in order to evaluate the possibility of providing services).
6. To ensure adequate provisions of the Services, the safety of information within the Services, as well as to improve, develop and maintain applications, technical systems and IT-infrastructure or our legitimate business interests, such as enabling us to improve and deliver a better and more personalised service	• Legitimate interest.	• Basic personal data; • Contact details; • Other personal data needed (in order to evaluate the possibility of providing services).
7. To provide an answer when you contact us through our website or other communication measures	• Your consent.	• Basic personal data; • Contact details; • Other personal data needed (in order to evaluate the possibility of providing services).

We do not process special category data related to your health, ethnicity, or religious or political beliefs unless required by law or in specific circumstances where, for example, you reveal such data while using the Services (e.g. in payments details).

The definitions used above are understood as follows:

Legitimate Interest: Okeo Payments legitimate interests are our business needs in conducting and managing our Services to create better benefits for our clients, increase the quality of our services, and at the same to ensure ours and our clients' interests.

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 Obligations: Processing your personal data where it is necessary for compliance with a legal or regulatory obligations that we are subject to.

Consent: Your consent shall mean any freely given, specific, informed and unambiguous indication of your wishes by which you, by a statement or by a clear affirmative action, signify your agreement to the processing of personal data relating to you. We can request from you a consent for processing when we do not have another legal basis for processing of your data.

If you provide us personal data about other people (such as your spouse or family) or you ask us to share their personal data with third parties, you confirm that you have brought this Policy to their attention beforehand.

How we obtain your personal data

We collect information you provide directly to us when you:

- Fill in any forms;
- Open a payment account or use any other of the Services;
- Correspond with us;
- Speak with a member of our Client support team;
- Contact us for other reasons.

We may collect personal data from third parties. In particular:

- We collect personal data from third parties such as public or private registers and databases. This includes information to help us check your identity, if applicable, information about your spouse and family, and information relating to your transactions;
- Occasionally we will use publicly available information about you from publicly available sources (e.g. media, online registers and directories) and websites for enhanced due diligence checks, security searches and other purposes related to Client due diligence processes;
- We may collect personal data when it is provided to us by a third party which is connected to you or is dealing with us, for example, business partners, sub–contractors, service providers, merchant and etc.;
- We may collect personal data from banks or other financial institutions in case the personal data is received while executing payment operations;
- We may collect personal data from other entities which we collaborate with.

Our identification tools

In order to perform your identity verification, we are using the services provided by our partner "Ondato UAB". The Service Provider takes the photo images or video records of your face and your ID document that you provide through a mobile application or a dedicated website using the camera. For more information on "Ondato UAB" please read its Privacy Policy.

"Ondato UAB" solution is used for comparing live photographic data or video record of yourself and your ID document, 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.

The result of the face similarity (match or mismatch) will be retained for as long as it is necessary to carry out verification and for the period required by anti-money laundering laws.

We ensure that your face similarity check is a process of comparing data acquired at the time of the verification, i.e. this is a one-time user authorization by comparing person's photos to each other. Your facial template is not created, recorded or stored. It is not possible to regenerate the raw data from retained information.

Using "Ondato UAB" services, personal data is used for your identification, since "Ondato UAB" verifies the identity of the person in the identity document and the person captured in the photo. This process shall allow us to verify your identity more precisely and make the process quicker and easier to execute. If you do not feel comfortable with this identification method you may contact us by email at hello@okeo.com for an alternative way to identify yourself.

Direct marketing

We may use our existing clients' email for our similar goods or services marketing. In case you do not object to the use of your email for the marketing of our similar goods and services, you are granted with clear, free of charge and easily realisable possibility to object or withdraw from such use of your contact details.

We may also provide the information to you, if being our client, about our products or services by sending the messages in the web-based platform and such messages may be viewed in the messages panel, 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 the 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 matters in relation to our business partners or other third parties on the legal basis for this, i.e. on the basis of your prior consent.

In case you do not agree to receive these marketing messages 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 email notification.

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.

For more information about your rights please see the section **Your rights**.

How we share your personal data

We sometimes need to provide your personal information to third parties for a better performance of our Services to you. These third parties (data processors) include:

- our external IT software providers (e.g. Mambu GmbH), in order to provide you with top-class payment solutions;
- communication services providers, in order to help us send you emails, push notifications and text messages;
- analytics providers and search information providers (e.g. Google Maps API refer for more details on Google Privacy Policy);
- infrastructure service providers (e.g. Google Cloud Platform services);
- supervising authorities (e.g. Bank of Lithuania, Financial Crime Investigation Service);
- people or companies that you transfer money to;
- other financial institutions, when you make outbound payments or receive payments;
- our lawyers or other external consultants, in order to perform activities required by law (e.g. internal or external audit);
- other entities or the personal data may be shared with them under the contract which is concluded between you and us;
- other entities under an agreement with us.

International transfer of personal data

In case your personal data is transferred outside the EEA, we will take necessary 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:

- 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;

- the recipient has signed or contains in its terms of the service (service agreement) standard data protection clauses which are approved by the European Commission;
- 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.

How we protect your personal data

The safety of your data is our top priority. You can be sure that your data is stored with utmost care. A variety of logical and physical security measures are used to keep your personal data safe and prevent unauthorized access, usage, or disclosure of it (the list indicated below is not exhaustive):

- Your personal data is stored in secured environment. Data is automatically encrypted prior to being written to disk. Each encryption key is itself encrypted with a set of master keys. Keys and encryption policies are managed the same way, in the same keystore, as for Google's production services;
- We use access control policies and segregation of duties which ensure that only restricted group of employees have access to your personal data. Staff is continuously trained about the importance of data safety and how to handle the data properly;
- Your password is kept in secured datastore, encrypted using BCrypt. BCrypt assigns a random number unique to each user, known as the "salt", that is then combined with the user password. Bcrypt then repeatedly uses a block cipher for a specific number of iterations on the combined "salt"+ password to generate a key. Password can't be deciphered without the key.
- All transactions you make through our platform after you log in are encrypted.
- HTTP Communication between your browser and our Services is secured using TLS 1.2 certificates,
- All data stored in our platform is a subject of back-up on ongoing basis.

While we take all the above steps to keep your data safe, you should take precautions to:

- Securely transmit your information to our web-based platform;
- Keep your credentials (e.g. login and password) e.g. for Okeo Payments web-based platform confidential and do not share it with anyone.

How long we keep your personal data

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 not 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 the Services and as required by the 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:

- 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;
- in case of the conclusion and execution of contracts – until the contract concluded between you and us remains in force and up to 10 years after the relationship between you and us has ended;
- 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;
- the personal data submitted by you through our website or via email 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:

- it is necessary in order for us to defend ourselves against claims, demands or action and exercise our rights;
- there is a reasonable suspicion of an unlawful act that is being investigated;
- your personal data is necessary for the proper resolution of a dispute/ complaint;
- under another statutory basis.

Your rights

The right to be informed. You have the right to be provided with clear, transparent and easily understandable information about how we use your personal data.

The right to access. You have the right to request from us the copies of your personal data. Where your requests are excessive, in particular if they are being sent with a repetitive character, we may refuse to act on the request, or charge a reasonable fee taking into account the administrative costs for providing the information. The assessment of the excessiveness of the request will be made by us.

The right to rectification. You have the right to request us to correct or update your personal data at any time, in particular if your personal data is incomplete or incorrect.

The right to data portability. The personal data provided by you is portable. You have the right to request that we transfer the data that we have collected to another organization, or directly to you, under certain conditions.

The right to be forgotten. When there is no good reason for us to process your personal data anymore, you can ask us to delete your data. We will take reasonable steps to respond to your request. If your personal data is no longer needed and we are not required by law to retain it, we will delete, destroy or permanently de-identify it.

The right to restrict processing. You have the right to restrict the processing of your personal data in certain situations (e.g. you want us to investigate whether it is accurate; we no longer need your personal data, but you want us to continue holding it for you in connection with a legal claim).

The right to object processing. Under certain circumstances you have the right to object to certain types of processing (e.g. receiving notification emails). However, if you object to us using personal data which we need in order to provide our Services, we may need to close your payment account as we will not be able to provide the Services.

The right to file a complaint with a supervisory authority. You have the right to file a complaint directly the State Data Protection Inspectorate of Lithuania 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://vdai.lrv.lt/lt/veiklos-sritys-1/skundu-nagrinejimas.

Rights related to automated decision-making. You have the right not to be subject to a decision which is based solely on automated processing and which produces legal or other significant effects. In particular, you have the right:

- to obtain human intervention;
- to express point of view;
- to obtain an explanation of the decision reached after an assessment; and
- to challenge such a decision.

Right to withdraw your permission. If you have given us consent, we need to use your personal data, you can withdraw your consent at any time. It will have been lawful for us to use the personal data up to the point you withdrew your permission

If you would like to exercise any of these rights, please contact us at our email: dpo@okeo.com. For security reasons, we will not be able to process your request if we are not sure of your identity, so we may ask you for proof of your ID.

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.

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.

Changes for this Privacy Policy

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.

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

Contact us

You may contact us by writing to us an email at hello@okeo.com or post us at Okeo Payments, UAB address Gedimino pr. 20, LT-01103, Vilnius, Lithuania.

Our Data Protection Officer

Our Data Protection Officer (hereinafter – DPO) continuously monitors our privacy compliance and communicates with us on data protection matters relevant to the provision of our Services. You may contact our DPO regarding all issues relating to our Company's processing of your personal data and the exercise of your data protection rights by sending an email to the address: dpo@okeo.com.