**PAYAPP DIGITAL, UAB**
**PRIVACY POLICY**

This Privacy Policy (hereinafter – the **Privacy Policy**) provides you with the basic information on how **PAYAPP DIGITAL, UAB**, a company registered in the Republic of Lithuania, legal entity code 305397637, registered address at Upės St. 23, Vilnius, the Republic of Lithuania, (hereinafter – **us** or the **Company**) processes your personal data.

Please read this Privacy Policy carefully. Should you have any questions regarding the processing of your personal data, please do not hesitate to contact us by e-mail data@payapp.com.

## 1. YOUR PERSONAL DATA CONTROLLER

1.1. The Company provides payment services while acting as an agent of GlobalNetint, UAB, a company registered in the Republic of Lithuania, legal entity code 304604766, registered address at Lvovo st. 25-104, Vilnius, the Republic of Lithuania, (hereinafter – **GlobalNetint**). GlobalNetint is an electronic money institution, authorized under the Law on Electronic Money and Electronic Money Institutions of the Republic of Lithuania and regulated by the Bank of Lithuania to carry out activities associated with electronic money, on-line payments and e-commerce.

1.2. The controller of your personal data processed in relation to the provision of payment services (as described in the Section 2 of this Privacy Policy) is GlobalNetint which independently sets the purposes and means of the processing of personal data related thereto. In such case, the Company is your personal data processor. You can find more information about the processing of personal data carried out by GlobalNetint in its privacy policy (https://globalnetint.com/render/GNI-Privacy-Policy.pdf?ver=1.2).

1.3. The controller of your personal data processed for the purposes other than closely related to the provision of payment services (as described in the Sections 3-5 of the Privacy Policy) is the Company which independently sets the purposes and means of the processing of personal data described in the abovementioned Sections of the Privacy Policy.

1.4. In all cases, whether acting as a data controller or a data processor, we apply Sections 7-10 of the Privacy Policy to all data subjects whose data we process and we aim to ensure data protection by implementing provisions of the General Data Protection Regulation (EU) 2016/679 and other personal data protection legislation.

## 2. PROVISION OF OUR SERVICES

***Personal data processed on the basis of agreements concluded (to be concluded) with our clients*** (hereinafter – the **Clients**)

2.1. Whereas the Company provides payment services as an agent of a licensed electronic money institution, the Company follows the provisions of the Law on Payments of the Republic of Lithuania and other legal acts. The Clients gain access to the services provided by the Company by entering into agreement with the Company.

2.2. When the Client expresses the will to use our services or starts using them, we will process personal data of the Client for the purpose of provision of our services on the legal basis of the agreement concluded (to be concluded) with the respective Client.

2.3. In order to grant access to our services, we may process the following data of the Client (and/or its representatives):

2.3.1. personal identity data (name, surname, date of birth, etc.);
2.3.2. contact details (address, telephone number, e-mail address, etc.);

2.3.3. financial data (payment account number, account balance, data about executed transactions, etc.);
2.3.4. other data provided by the Client (and/or its representatives) and data relating to our services.

2.4. We may obtain personal data of our Clients directly from them and from third parties, including financial institutions, entities providing identification services, public registers, databases, social networks, etc.

2.5. Please note that the processing of all the aforementioned data is necessary for the provision of our services. If we do not receive the aforementioned data (or any part thereof), we will not be able to properly provide payment services.

2.6. When providing our services, we will process personal data of our Clients for up to 10 years from the date of the of termination of the agreement on provision of the payment services with the respective Client, unless a longer period of retention of individual data is required by law.

***Access to the individual Client account***

2.7. Each Client uses our services by logging into individual account through the website www.payapp.com (hereinafter – the **Website**). The Company creates unique login credentials to each Client in accordance with the agreement on provision of payment services entered into by the Company and the Client.

2.8. In order to properly provide payment services, the Company processes unique login credentials (username, password, etc.) as well as information about the Client's activity on the individual account accessible through the Website. Such information is processed on the legal basis of the agreement concluded (to be concluded) with the respective Client.

2.9. The processing of login credentials and information about Client's activity on the account accessible through the Website is an essential part of the services provided by the Company. Therefore, such data processing is necessary for the provision of our services. If we do not process the aforementioned data (or part thereof), we will not be able to properly provide our services.

2.10. We will process login credentials and information about Client's activity on the account accessible through the Website for up to 5 years from the date of the of termination of the agreement on provision of the payment services with the respective Client, unless a longer period of retention of data is required by law.

***Prevention of money laundering and terrorism financing***

2.11. The Company processes the personal data of the Client (and/or its representatives/beneficiaries) while acting in compliance with the requirements set in the provisions of the Law on Prevention of Money Laundering and Terrorism Financing of the Republic of Lithuania (hereinafter – the **Law**).

2.12. Before starting any business relations, the Company shall establish the identity of its Clients, their representatives and beneficiaries. The processing of such personal data is mandatory and the legal ground for such processing is legal obligation laid down in the Law.

2.13. The Company may process the following personal data of the Client (and/or its representatives/beneficiaries) for the purpose of prevention of money laundering and terrorism financing:

2.13.1. personal identity data (name, surname, date of birth, data from an identity document and a copy of the document, etc.);
2.13.2. contact details (address, telephone number, e-mail address, etc.);
2.13.3. visual data (photo, direct video transmission (direct video broadcast) recording, etc.);
2.13.4. data about activities (current activity, current public function, etc.);

2.13.5. financial data (payment account number, account balance, data about executed transactions, etc.);
2.13.6. other data provided by the Client (and/or its employees/representatives/beneficiaries) and data required by the Law.

2.14. The personal data required under the Law are usually provided to us directly by the Client. However, the Company shall also have the right to establish the identity of the Client and/or its representatives/beneficiaries without their direct involvement by receiving the required information from other financial institutions and authorized entities in accordance with the procedure laid down in the Law.

2.15. For the purpose of prevention of money laundering and terrorism financing personal data shall be stored by us in compliance with the requirements of the Law, i.e. for a term of 8 years from the date of termination of transactions or business relations with the Client. In certain cases stipulated by the Law, some personal data shall be stored for a shorter period of time (for example, correspondence related to business relations with the Clients shall be stored for a term of 5 years).

## 3. SUBMITTING REQUESTS

3.1. To ensure timely and appropriate processing of your requests, protect our interests and interests of our Clients and fulfil various legal requirements, we process your personal data when you contact us (by e-mail, through our Website, social media accounts or by any other method) irrespective of your relationship with the Company or absence thereof. We may also record conversations with you (over the phone, Skype or other remote ways). We store all communications with you to ensure that in case of disputes we have all available communication logs.

3.2. When your request is related to the agreement on provision of payment services concluded/to be concluded with you, the basis for the processing of your personal data upon your request is such agreement on provision of payment services. In this case, your personal data is processed in accordance with the Clauses governing processing of personal data on the basis of agreements concluded (to be concluded) with our Clients (Clauses 2.1- 2.6) and the Clause 1.2 of the Privacy Policy shall be also applied.

3.3. In cases other than specified in the Clause 3.2 (i.e. when your request is not related to the agreement on provision of payment services concluded/to be concluded with you) the basis for the processing of your personal data is consent which is expressed through your active actions – submitting a request. In this case, your personal data is processed in accordance with the Clauses of this Section 3 and the Clause 1.3 of the Privacy Policy shall be also applied.

3.4. We store your personal data for the aforementioned purposes for up to 3 years, depending on the nature of received personal data and other circumstances. We apply longer periods of personal data storage when:

3.4.1. there is a reasonable suspicion of an unlawful act which is subject to investigation;
3.4.2. your data is necessary for the proper resolution of the dispute, complaint or claim;
3.4.3. we have received complaints related to you, or we have noticed any violations committed by you;
3.4.4. it is necessary for back-up copies or related purposes of functioning of our internal systems;
3.4.5. it is mandatorily required by applicable law;
3.4.6. etc.

3.5. In any case, we recommend protecting your personal data when submitting the requests and not disclosing the personal data if such disclosure is not necessary in the context of your request.

## 4. MARKETING

4.1. Our legitimate interest is to provide you with accurate information about the services we provide, extra services, etc., so if you agree with our T&C or give additional clear consent (e.g., in a manner of additional tick box to be ticked with a link to the Privacy Policy and / or other relevant documents), we shall process your personal data for marketing purposes – for the purpose of providing customized advertisements and sponsored content and sending promotional communications; assessment and analysis of our market, clients, products and services (including asking for your opinions on our products and services and carrying out client/partner surveys). We will provide you information on the progress of Company's projects, updates, news and other relevant information regarding services provided by the Company.

4.2. In this case, the Company shall process your personal data such as name, social media account details, telephone, e-mail, address, your interest.

4.3. Your personal data processed for marketing purpose shall be stored for 3 years from your last visit to our website unless you withdraw your consent before the expiry of this period or repeatedly give a consent. Upon the expiry of this period or upon your withdrawal of consent, the Company shall stop processing your personal data.

4.4. You shall have the right to unsubscribe from newsletters sent to you at any time. You can unsubscribe from newsletters by clicking on the dedicated link at the bottom of the newsletters sent to you or by notifying the Company in writing (for example, by e-mail). If you received the marketing content from us and know/ think that your additional consent had not been provided to us, then please inform us about this situation as soon as possible via data@payapp.com

4.5. If you are the Client of the Company, we may send you direct marketing messages by e-mail providing you with relevant information about other (related) services provided by the Company. You may opt-out of these messages at any time (in advance or at any time thereafter) by clicking on the dedicated link at the bottom of the newsletters sent to you or by notifying the Company in writing (for example, by e-mail).

## 5. VISITING OUR WEBSITE

5.1. When you browse our Website, we do not hold any personal data about you, but we use various tools to help us maintain the Website and provide the best possible experience for you.

5.2. Each time you access or visit the Website, the following technical personal data may be automatically collected: IP address, access date and time, webpage name and URL, device operating system data, information about the Internet provider, geo-location data, language settings and other relevant data.

5.3. We may also collect and use cookies. Cookies are a small piece of information saved in your browser storage. They help us to recognize you as a visitor having previously visited the Website, to save your browsing history and to customize the content accordingly. Cookies also help to ensure a smooth operation of the Website, to monitor the duration and frequency of visits to the Website and to collect statistics on the number of visitors to the Website. For further information, please see PAYAPP's Cookies Policy .

## 6. AUTOMATED DECISION MAKING AND PROFILING

6.1. Your data may be processed both automatically and by physical means, which includes automated decision making and profiling for different processing purposes.

6.2. Automated decision making and profiling may be used to verify your identity, verify data in international databases, track your operations and transactions, activities, assign you to certain categories, assess your risk, anticipate other aspects. Such actions are mandatory under the current anti-money laundering and counter-terrorist financing regulations and are necessary when starting a business relationship with the Client. For these reasons, you shall not have the right to opt out of automated decision making, including profiling. Nevertheless, you shall have the right to request human intervention, state your

position, receive a more detailed explanation of the decisions made following this assessment, and the right to challenge such decision.

## 7. SECURITY OF YOUR DATA

7.1. We take protecting of your personal data very seriously and strive to apply all necessary organizational and technological security measures.

7.2. In order to protect your personal data:

7.2.1. we ensure that access to your personal data is granted only to those employees who require it in the provision of our services and are familiar with security requirements, employees' duties and responsibilities;
7.2.2. we use technological tools to protect your personal data: intrusion detection and prevention systems, DOS attack protection systems, firewalls, personal data encryption, real-time security event analytics, and other advanced security technologies;
7.2.3. we encrypt your personal data in the server thus protecting it against disclosure;
7.2.4. electronic information security is monitored by cyber security professionals;
7.2.5. information systems security is tested periodically;
7.2.6. we constantly back up personal data and keep it away from key information in order to protect your data from loss (such as computer system malfunctions). We also ensure that backups are at least as secure as the underlying data. We regularly test our backups to make sure we are prepared for emergencies;
7.2.7. our premises are protected by technical, electronic and physical security measures;
7.2.8. we continuously educate our employees on information security so that we can identify personal data threats and protect against them in a timely manner.

7.3. While we implement different security measures, you should be aware that complete and absolute security is not always possible, and we cannot guarantee the security of any information you disclose online. By browsing the Website and/or using the services of the Company you expressly acknowledge and agree that any personal information or other data provided by you to us or third persons is provided at your own risk.

## 8. RECIPIENTS OF YOUR PERSONAL DATA

8.1. We may contract (hire) certain service providers, i.e. data processors, to process your personal data. These may be companies providing data storage, server and/or communication services, companies developing and maintaining software, companies providing marketing services and analysis of activities online, online traffic and website analysis, statistics services and other service providers. Your personal data may be transferred to these data processors only when and solely to the extent necessary for the provision of the respective services of these data processors.

8.2. We may share your personal data with other members of the group of companies to which the Company belongs for purposes consistent with this Privacy Policy.

8.3. We may also transfer certain personal data to third parties, such as courts, persons providing legal or audit services, in compliance with legal requirements, lawful instructions from competent authorities, and other individuals in the performance of legislative requirements, legitimate instructions by competent authorities or on the basis of another legitimate basis.

8.4. Usually, we do not transfer personal data outside the European Economic Area (EEA). However, in some cases, the performance of our activities may require transfer of your personal data to a data recipient outside the EEA (e.g. if our service provider is located outside of the EEA) to a certain extent. In this case, we shall aim to ensure that the security measures required for such data transfer are implemented (e.g. that a US based data recipient has been certified in accordance with the EU and US privacy

requirements; that the data recipient has been certified in accordance with the European Commission as properly).

## 9. YOUR RIGHTS AS A DATA SUBJECT

9.1. General Data Protection Regulation (EU) 2016/679 gives you more rights to control your data processing. Here is a list of rights specified in the regulation:

9.1.1. the right of access to your personal data. You have the right to receive confirmation that we process your personal data as well as the right to access your personal data processed and information about the purposes of processing, the categories of data being processed, the categories of data recipients, the period of data processing and the sources of data;

9.1.2. the right of rectification. If you think that data processed by us is inaccurate or incorrect, you have the right to request that such data be modified, clarified, corrected or disregarded;

9.1.3. the right of erasure (right to be forgotten). When there are circumstance specified in legal acts, you have the right to request us to erase your personal data;

9.1.4. the right of restriction of processing. When there are circumstances specified in legal acts, you also have the right to request us to restrict the processing of your personal data;

9.1.5. the right of data portability. You have the right to transfer your data processed by us with your consent and by automated means to another data controller;

9.1.6. the right to disagree with the processing of your persona data if it is processed on a legitimate interest basis, unless there are legitimate reasons for such processing or for the purpose of claiming, enforcing or defending legal requirements;

9.1.7. the right to revoke your consent to process your personal data. If we have no other legal basis for the processing of personal data, we will cease processing of personal data immediately after the cancellation/revocation of the consent provided by you.

9.2. These rights of data subjects shall be implemented if all requirements set by applicable legal acts are met. In order to exercise your rights, contact us by e-mail at data@payapp.com. Having received your written request, we may ask you to confirm your identity and/or to revise the scope of the implementation of your specific right as a data subject.

9.3. Finally, if you feel that your personal data protection rights have been violated, you shall have the right to contact the State Data Protection Inspectorate (www.vdai.lrv.lt) in all cases and to lodge a complaint. However, we recommend that you contact us prior to a formal referral to the supervisory authority to find a mutually appropriate and effective solution to the problem emerged.

## 10. FINAL PROVISIONS

10.1. We have the right to adjust the provisions of this Privacy Policy. In such case, we will notify you of any changes of the Privacy Policy in advance and will publish a new version of the Privacy Policy on our Website. The Privacy Policy was last amended on 20 June 2020.