PRIVACY POLICY

I. INTRODUCTION

This Privacy Policy outlines how SharPay (“SharPay”, “we”, “our”, “us”), collects, uses, stores, shares, and protects your personal data. This Privacy Policy is addressed to all individuals who are current, past, or potential customers of Sharpay and policy applies when you use our services via our website, mobile applications, payment cards, or any other related services provided by SharPay. By using our services, you acknowledge and agree to the terms of this Privacy Policy.

Please read this Privacy Policy carefully. It is part of our Terms of Service. We may update this Privacy Policy from time to time, and we will notify you of any significant changes by posting the updated policy on our website and sending an email if necessary. Continued use of SharPay services after such changes indicates your acceptance of the revised Privacy Policy.

2. LEGAL INFORMATION AND DATA CONTROLLER

We collect, process, and store your personal data based on the legal grounds established by applicable data protection laws, including the General Data Protection Regulation (GDPR, EU Regulation 2016/679) and Personal Information Protection and Electronic Documents Act (PIPEDA).

Data Controller means anyone who alone or jointly with others determines the purposes and means of the processing of Personal Data. For the purposes of GDPR, the SharPay will be the “Controller” of the personal data you provide to us.

Depending on the services you use SharPay refers to the one from the following companies (“Company”):

SPEKA PAYMNETS CORP., incorporation number BC1383565, registered at 5577 153A Street, Suite 207, Surrey BC V3S 5K7, CANADA, is a registered provider of money service business (MSB), regulated by the FINTRAC Canada, MSB registration number: M22046940

GTM EXCHANGE LTD, incorporation No. HE 348749, registered at Parodos Acheritou, 1, Erimi 4630, Limassol, Cyprus.

FLEX EXCHANGE SOLUTION UAB, incorporation No. 305965171, registered at Laisvės pr. 60, Vilnius 05103, Lithuania.

Privacy related questions may be addressed to SharPay Data Protection Officer by sending an e-mail to support@sharpay.net.

3. BASIC PRINCIPLES THAT SHARPAY ADHERES TO IN RELATION TO YOUR PERSONAL DATA

- We are committed to ensuring that your personal data is processed lawfully, fairly, and transparently.

- We only collect personal data for the specific purposes outlined in this Privacy Policy and will not process it further in ways that are incompatible with those purposes.
- We will take all reasonable steps to ensure that your Personal Data is accurate and, where appropriate, kept up to date.
- Your personal data will be stored in a form that allows identification only for as long as necessary to fulfill the purposes for which it was collected. This is in line with our Information Security and Data Storage Policy, ensuring that we store and process your data securely.
- We implement appropriate technical and organizational measures to safeguard your Personal Data from unauthorized access, unlawful processing, accidental loss, alteration, or destruction.
- Personal data may be stored and processed securely within the EU or in a location specified in the agreements we enter with you. We may also use authorized third-party processors to handle personal data, ensuring they process data based on our written instructions, in compliance with applicable laws, and with adequate security measures.
- In cases where Personal Data is necessary to fulfill an agreement or comply with legal obligations, failure to provide such data may prevent us from delivering our services to you.

4. PERSONAL DATA WE COLLECT

What is Personal Data

For the purposes of this Privacy Policy, the terms "personal data" and "personal information" are used interchangeably and shall have the meanings described in the relevant acts and regulations. GDPR (EU Regulation 2016/679) defines "personal data" as any information that relates to an identified or identifiable living individua. Under PIPEDA, “personal information” includes any factual or subjective information, recorded or not, about an identifiable individual.

What Personal Data we collect

When you apply to become a SharPay customer, we will request certain personal information to verify your identity and manage your account. The specific information required will depend on the type of product you are applying for, but it will generally include the following:

Identification Data: This includes name, surname, personal identification code, place and date of birth, citizenship, identification document details (such as a copy of the passport or ID card, date and country of issue, expiration date, document number, issuance authority), photo, and signature.

Contact Data: This includes phone number, email address, residential address, and language of communication.

Financial Data: This includes account number, transaction details (including incoming and outgoing payments), transaction history, loan obligations, other financial obligations, and accounts held at other financial institutions.

Tax Residence Information: This includes country of residence, country of tax residence, taxpayer identification number (TIN), and citizenship.

Professional Activity Data: This includes the Customer’s place of work, profession, position, occupation, length of service, and education.

Communication Data: This includes data collected when the Customer communicates with SharPay via telephone, visual and/or audio recordings, email, messages, and other communication channels (including social media). It also includes data related to the Customer's visit to SharPay's website or communication through other SharPay channels (such as chat).
KYC Data: This includes data related to the Customer's due diligence, including relationships with legal entities for executing transactions on behalf of the entity, legal representatives (acting with relevant authorization or otherwise), contracting parties, and contract participants. It also includes information about the Customer's funds and sources of wealth, ultimate beneficial owners (UBOs), company directors, shareholders, share ownership, management board members, and any self-declarations regarding politically exposed persons (PEP). KYC data also includes information available from public registers, social networks, screenings against sanction lists, PEP status, and data on the origin of assets and wealth.
Public Register Data: This includes data obtained from public registers or created while fulfilling legal obligations or as a result of inquiries made by investigative bodies, notaries, tax administrators, courts, and bailiffs. This may include details of income, credit commitments, property holdings, and debt balances.
Your device and location Data: This includes Internet Protocol (IP) address, handset ID, log-in information, browser type and settings, time zone, the operating system, the type of device you use, a unique device identifier, screen size, mobile network information, mobile operating system and type of mobile browser you are using, date, time and length of your visit

How we collect Personal Data
We obtain personal data from a variety of sources:
Directly from you: When you provide information to us directly, such as when registering for our services, completing forms, setting up and using your SharPay account, making transactions, or subscribing to communications from us.
From your representatives: If you are a beneficial owner, shareholder, representative, or employee of a corporate client, your personal data may be provided to us by the representatives of the company you are associated with. This data is processed in line with legal and regulatory obligations, and you retain all the rights associated with your data under applicable laws.
From third parties: We may receive personal data from third parties with whom you have dealings, such as business partners, service providers, fraud prevention agencies, and others involved in transactions. Additionally, we may collect data to assist with regulatory checks, including from financial institutions, or for compliance with "Know Your Customer" (KYC) requirements.
From publicly available sources: We may also gather information from public sources, such as government registers and databases, open websites, or other public domain data, to ensure the accuracy of our records and improve our services.

5. HOW WE USE PERSONAL DATA
We process your personal data only where a lawful basis exists. We make every effort to limit the amount of information we hold about you and use it only when necessary. Therefore, the legal basis and related purpose for each processing activity will be one of the following:

Performance of a Contract. We process your personal data to provide you with the services you request and to manage your SharPay account. This includes actions necessary to enter into, execute, and terminate agreements with you, such as setting up your account, managing transactions, and processing payments. Additionally, we use your data to ensure secure access to your account, including sending one-time passwords or other access codes. We may also share your data with third-party providers to offer services like issuing cards or processing wire transfers.
We may also use your data to send you important notifications, such as account confirmations, alerts about suspicious activity, and transaction updates, as well as to provide customer support when you contact us.

Compliance with Legal Obligations. We process your personal data to comply with our legal obligations, particularly in relation to anti-money laundering (AML) and combating the financing of terrorism (CFT) regulations. This includes verifying your identity as part of the Know Your Customer (KYC) process, and sharing your data with relevant service providers for compliance. We may also disclose data to law enforcement or as required by a court order to meet legal obligations.

Legitimate interests. We process personal data to protect our legitimate interests if these interests do not conflict with your legal rights and freedoms. We process anonymized and aggregated data to analyze how customers use our services, improve the quality and functionality of our platform, and enhance customer experience; to prevent, limit and investigate any misuse or unlawful use or disturbance of the services; 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. This includes troubleshooting, data analysis, testing, and research to refine our services and resolve any technical issues. Additionally, we use your data to notify you about important updates, such as changes to policies or new features. We also assess user profiles and transactions to detect and prevent fraudulent activities and to protect both our and your interests. When you contact customer support, we may record and retain the details of the conversation. This helps us improve our services, resolve any disputes, and ensure quality service through employee training.

Your Consent. In some cases, we may ask for your consent to process your personal data. For example, we may ask for your consent to send you marketing emails or to analyze your use of our products. You may withdraw your consent at any time. For account verification, we may ask you to complete a liveness test to confirm your identity. This involves using your camera to capture specific facial features, which constitutes processing of special category personal data and can only be done with your consent. This process is carried out by a third-party service provider acting on our behalf.

If you initiate a conversation with our customer support service, you may be asked to provide additional information about yourself and your transaction. Also, our customer support service may contact you to request additional proof of your identity, such as a new or updated image of your identity document and/or a scanned copy of the front of a payment card to verify that

your transaction is valid, or to the extent that it may be necessary to comply with our legal obligations.

6. HOW WE PROTECT YOUR DATA

At SharPay, we are committed to ensuring the security of your personal data. We have implemented a variety of technical and organizational measures to provide an appropriate level of protection, including physical, technical, and administrative safeguards. These measures are designed to reduce the risks of data loss, misuse, unauthorized access, disclosure, or alteration by third parties.

To keep your data safe, we use the following measures:

- We encrypt both the transmission and storage of your personal data using the highest standards of technology and security protocols. This ensures the integrity and confidentiality of your data.
- We have systems in place to detect any unauthorized access attempts to our data.
- The locations where your data is stored are protected with round-the-clock security, and we enforce strict access controls to prevent unauthorized personnel from gaining physical access.
- Only authorized employees have access to the physical and digital systems containing your personal data, and they are verified before being granted access. We ensure that all employees who have access to your personal data are subject to non-disclosure agreements, and we limit access to only those employees whose job functions require it (e.g., customer support staff). Additionally, we conduct ongoing training to maintain the security and confidentiality of personal data.
- All service operations are conducted with stringent safety procedures to safeguard your personal data.
- To further protect your personal data, we impose the same data protection obligations on our subcontractors, partners, and service providers as set out in our contractual agreements with them.

To ensure your own safety, we recommend you follow best practices for securing your account. This includes using strong, unique passwords with a mix of letters, numbers, and symbols, and never sharing your wallet password with anyone. Please note that SharPay employees will never ask for your password.

Additionally, we recommend that you always sign out of your SharPay account when you're finished using it, especially on shared or public devices. You are responsible for any loss or misuse of your account due to the sharing of your password or failure to follow these guidelines.

Although we take all reasonable precautions to protect the data we process, it is important to note that no system or electronic data transmission is completely secure. We continuously monitor our systems 24/7, and our staff is always ready to respond quickly to any notifications or queries you may have regarding your data.

Our goal is to continuously improve our security practices to meet the highest industry standards and provide the best protection for your data.

7. HOW WE SHARE YOUR DATA

Your Personal Data remains under our control, and we warrant that SharPay will not disclose your personal data to unauthorized third parties. However, we may share your data in specific situations where required for the actions you take or to fulfill our regulatory or legal obligations. Any data transfer occurs only between us and third parties with whom we have agreements to ensure the protection and confidentiality of your data.

We may share your data with the following recipients:

- Supervisory and other regulatory and government authorities, such as the Central Bank of Cyprus, the European Central Bank, the Bank of Canada, the Bank of Lithuania, tax authorities, MOKAS, prosecution authorities, and financial crime investigation services like the FCIS in Lithuania.
- External legal consultants or auditors.
- Credit or financial institutions that may be involved in executing your payment orders or transfers, including our partners like Walletto UAB.
- Card issuing companies and processing companies if you choose to order our card products.
- File storage companies, archiving, and/or records management companies, and cloud storage providers.
- AML analytics and KYC service providers.
- Other business partners, suppliers (including but not limited to IT suppliers, card manufacturers, delivery services, etc.) and affiliates.
- Potential investors in our business.

Given the global nature of financial services in some cases, your personal data may be transferred to third countries outside the European Economic Area (EEA) or Canada. This may occur, for example, to process your payment orders or if such transfer is required by law, such as for tax reporting obligations. When transferring personal data to third countries, we ensure that the recipients comply with Canadian and European data protection standards, implementing appropriate security measures in line with the GDPR and PIPEDA.

8. HOW LONG WE KEEP YOUR DATA

SharPay will not retain your personal information for longer than is necessary for the actions described in this Policy unless a longer retention is required by law. Information collected under AML laws requirements as well as transactions' history shall be kept for 8 years after you close your account. Provided data retention timeline can be extended for up to 2 (two) years upon reasoned instruction of a competent authority. When your personal data is no longer needed and/or the term prescribed by law expires, we securely delete your data.

Any personal data that We use for marketing purposes will be stored until you notify us that you no longer wish to receive this information.

9. YOUR RIGHTS

With certain exceptions and depending on the type of data processing we conduct, you have specific rights concerning your personal data. Each user is entitled to the following rights:

- You have the right to request a copy of the information we hold about you. If you would like to receive a copy of some or all of your personal data, please email us at support@sharpay.net. We will provide you with this information free of charge within 30 (thirty) days.
- You have the right to request that your personal data be deleted, unless there are additional legal and/or regulatory requirements that prevent us from doing so.
- You have the right to data portability. To the extent that we process your personal data (i) based on your consent or in accordance with contractual obligations, and (ii) by automated means, you have the right to request the transfer of your personal data to another organization, if technically feasible, or directly to you in a structured, commonly used, machine-readable format.
- You have the right to ensure that your personal data is accurate and up to date, or to request corrections if necessary. If you believe your personal information is incorrect or incomplete, please contact us at support@sharpay.net.
- You have the right to restrict the processing of your personal data, for example, for direct marketing purposes.
- You have the right to object to any decisions based solely on automated processing of your personal data.
- If you believe that your rights have been violated, you may file a complaint to the to the Office of the Privacy Commissioner of Canada (https://www.priv.gc.ca/en/) or if you are in the EU, you can find the relevant supervisory authority on the European Data Protection Board website (https://edpb.europa.eu/about-edpb/board/members_en). Alternatively, you may file a complaint with the supervisory authority in your country of residence, place of work, or where the alleged violation occurred.
- You have the right to withdraw your consent at any time. If the processing of your personal data is based on consent, you can withdraw that consent at any time. Your withdrawal does not affect the lawfulness of processing based on consent prior to its withdrawal.
- You have the right to rectification, meaning you can request that we correct any information about you that you believe is inaccurate. Additionally, you have the right to request complete information about any data we hold about you that you believe is incomplete.

10. CHANGES TO THIS PRIVACY POLICY

We may revise and update this Privacy Policy periodically. In the event of any material changes, we will notify you and update the relevant version on our website.

11. CONTACT

Questions, comments and requests regarding our Privacy Notice are welcomed and should be addressed to our Data protection officer at support@sharpay.net

If you would like to make a complaint about the way we process your personal data please do it by sending an e-mail to support@sharpay.net. We will reply to your request within 30 days once we receive it. If we expect that responding to you will take longer, we will let you know.

12. USE OF COOKIES

We use cookies on our website. It allows us to determine if you are logged in or not and temporarily store non-personal data that is necessary for the correct operation. For information on what cookies are and how we use them, please refer to our Cookies Policy (https://srv001.fx-people.com:7443/files/en/Cookies_policy_SharPay.pdf)

13. DATA LOCATION

We use servers located in the European Union to store personal data. Also, if We share your data with a third party, including our related partners and/or affiliates, as described in this Privacy Policy, these third parties may be located outside of our usual location and your country of residence. In all such cases, the transfer of data will only take place after we ensure that the third party provides comparable levels of data protection and that they will only use your data for the purposes set out in this Policy

14. CHILDREN'S PRIVACY

We do not process personal data from children under the legal minimum age in accordance with the local legal requirements of the state, province, country, or jurisdiction of residence. We take appropriate steps to prevent children from using the Services. If you find that a minor child has provided us with personal data, please contact us at support@sharpay.net