Privacy Policy

Effective date: 01.03.2020

In this Privacy Policy (hereinafter – the Policy) you will find general principles of processing personal data including what information Wallester AS (hereinafter – the Wallester) collects about you, what we do with it and when we disclose it to others. Specific details on the processing of personal data might be also included in agreements entered or to be entered between you and Wallester and are reflected in Wallester app (hereinafter the App) and/or on our website www.wallester.com (hereinafter – the Website).

Wallester ensures, within the framework of applicable law the confidentiality of your personal data. For this purpose, Wallester has implemented appropriate technical and organizational measures to protect your personal data and for providing the transparent data protection rules.

Wallester has the right at any time and regularly improve or make changes to this Policy. Wallester will inform you about any changes in the App and/or on the Website, as well as by informing you individually.

1. Your personal data

1.1. What personal data does Wallester collect about me?

The personal data, which Wallester collects and processes includes the following:

Personal Data – your personal details and contact data, including full name, date of birth, personal identification code, citizenship, residency, residential address, tax residency, e-mail address, mobile phone number, occupation, identification document data, photo and/or video footage which you have forwarded to Wallester for the purpose of identifying yourself.

Due Diligence Data – Data which Wallester collects for the purpose of conducting due diligence under applicable anti-money laundering laws from you and appropriate databases.

Transaction and Payment Card Data – Details of any transfers made to and from Payment Account, including the name and account number of the payer and the payee, the date, time, currency, amount and explanation of the transaction, merchants' and ATMs' locations, payment card's number, the name on payment card, the expiry date of payment card and the CVV number of payment card.

Device Data – Information regarding the device on which you are using the App and/or Website, including the device's model, name or any other identifier and the IP address of the network from which you are using the App and/or Website, including location information.

Preference Data – Your preferences in the App and/or on Website (language preferences, transaction limits, etc).

Customer Support Data – Communication between you and Wallester customer support (telephone conversations, e-mails and chats).

Other Data – Other data not listed above, which is generated as a result of using the App and/or Website.

1.2. What are Wallester legal purposes and basis for using my personal data?

Wallester collects and processes your personal data for the following purposes:

Compliance Purposes – to perform an obligation under applicable laws, including the obligation to:

- avoid money laundering, terrorist financing and fraud;
- ensure the fulfilment of international financial sanctions;
- ensure the security of payment services;
- provide tax authorities data as required under tax information exchange laws;
- comply with the lawful inquiries and orders of public authorities with whom Wallester is obliged to cooperate under applicable laws, such as courts, bailiffs, trustees in bankruptcy, the police, financial supervisory authorities, financial intelligence units, tax authorities, etc;
- other financial institutions with whom Wallester is obliged to cooperate under applicable laws, including, upon your prior authorization, payment information service providers and payment initiation service providers.

Contractual Purposes – to perform or enter into an agreement between you and Wallester.

Fraud Monitoring Purposes – to monitor and prevent payment fraud.

Analytical Purposes – to gain a better understanding of the preferences of Wallester's customers and how do customers interact with the App and/or Website.

Marketing Purposes – to provide you marketing offers of Wallester's services and additional features.

Wallester collects and processes your personal data on the following legal basis:

Keeping to our contracts and agreements with you – we need certain personal data to provide our services and cannot provide them without this personal data.

Legal obligations – in some cases, we have a legal responsibility to collect and store your personal data (for example, under anti-money laundering laws we must hold certain information about our customers).

Legitimate interests – we sometimes collect and use your personal data, or share it with other organizations and/or institutions, because we have a legitimate reason to use it and this is reasonable when balanced against your right to privacy.

Consent – where you have agreed to us collecting your personal data (for example marketing purposes etc.).

1.3. Does Wallester process my personal data for profiling or automated decision making?

Wallester does not process your personal data for automated decision making. Wallester is, however, obliged under law, to assess the risk of money laundering, terrorist financing and fraud associated with you and your transactions. This assessment is partly conducted by automated means and involves profiling. If Wallester makes an automated decision about you, you will have the right to ask to review it manually by a person.

2. Your rights

2.1. What are my rights?

In connection with the processing of your personal data, you have the following rights:

Right to Information – you have the right to receive the information provided in this Policy. The valid version of this Policy will be available in the App and/or on the Website at any given time.

Right to Access – you have the right to ask Wallester to provide you a copy of your personal data which Wallester processes.

Right to Rectification – you have the right to ask Wallester to rectify your personal data in case the data is incorrect or incomplete.

Right to Erasure – you have the right to ask Wallester to delete your personal data, unless Wallester is obliged to continue processing your personal data under law or under the agreement between you and Wallester, or in case Wallester has other lawful grounds for the continued processing of your personal data. Wallester will, in any case, delete your personal data as soon as it no longer has lawful grounds for processing your personal data.

Right to Restriction – you have the right to ask Wallester to restrict the processing of your personal data in case the data is incorrect or incomplete or in case your personal data is processed unlawfully.

Right to Data Portability – you have the right to ask Wallester to provide you or, in case it is technically feasible, a third party, your personal data, which you have provided by yourself to Wallester and which is processed in accordance with your consent or under the agreement between you and Wallester.

Right to Object – you have the right to object to processing your personal data in case you believe Wallester has no lawful grounds for processing your personal data. For any processing conducted in accordance with your consent, you can always withdraw your consent.

Right to File Complaints – you have the right to file complaints regarding processing your personal data.

2.2. How do I exercise my rights?

To exercise any of your rights set out in the previous section, you may contact us by e-mail at dpo@wallester.com. For security reasons, we can't deal with your request if we are not sure of your identity, so we have the right to ask you for proof of your ID.

Wallester will make its best efforts to respond to your application within 1 week. Under GDPR art 12 (3) Wallester must respond to your application within 1 month. In case it is necessary due to the number and complexity of applications filed with Wallester, Wallester may, under GDPR art 12 (3), also respond to your application within 3 months.

3. Wallester and your personal data

3.1. Does Wallester share my personal data with anyone else?

Upon processing your personal data, Wallester may share elements of your personal data with the following third parties:

Public authorities and other financial institutions to whom Wallester is obliged to disclose your personal data under law;

Server hosts who are hosting Wallester's servers;

Payment processors and payment network operators who are processing your transactions;

Identification service providers who are helping Wallester to verify your identity and acquire Due Diligence Data;

Payment Card manufacturers who are manufacturing your payment card;

Communication service providers who are facilitating the e-mails, calls, SMS messages and other communication between you and Wallester;

Couriers who are helping Wallester to deliver letters (e.g. letters with your payment card and PIN codes) to you;

Other parties who are involved with the provision of Wallester's services.

The partners listed above may be located within and outside of the European Economic Area.

3.2. How does Wallester protect my personal data?

We use a variety of physical and technical measures to keep your personal data safe and prevent unauthorized access to or use or disclosure of it. Electronic data and databases are stored on secure computer systems with control over access to information using both physical and electronic means. Our staff receives data protection and information security training. We have detailed security, IT infrastructure use and data protection policies, which are based on the need-to-know and less-privileged access principles. Wallester staff are required to follow the policies when they handle your personal data.

We encrypt personal data, deploy firewalls, intrusion detection and prevention systems to ensure that all your personal data is confidential and safe. While we take all reasonable steps to ensure that your personal data will be kept secure from unauthorized access, we cannot guarantee it will be secure during transmission by you to our App, to the Website or other services. We use HTTPS (HTTP Secure), where the communication protocol is encrypted, for all - the Wallester App, the Website and the payment-processing services. We regularly test our system and review applicable policies to make sure that our IT safety measures are one step ahead of any threat.

If you use a password for the Wallester App and/or Website, you will need to keep this password confidential according to General Terms. Please do not share it with anyone.

3.3. How long will Wallester keep my personal data for?

According to anti-money laundering laws or with regard to Tax Residency Data under relevant tax information exchange laws we generally keep your personal data for 5 years from the end of financial year when

relationship between you and Wallester was terminated and your payment account was closed. Upon Estonian Financial Intelligence Unit request this period may be extended up to another 5 years. Such period may be longer as may be required by applicable local laws, for example, the transaction data what is stored by Wallester for 8 years from the end of financial year when relationship between you and Wallester was terminated and your payment account was closed. We may keep your personal data for longer because of a potential or ongoing court claim or another legal reason.

After the periods stipulated in this Section above Wallester will delete your personal data.

3.4. Does Wallester use cookies on Wallester Website?

Wallester uses cookies to analyze how you use our website. Please read the Cookies Policy for more information about cookies.

3.5. Who is the data controller of my personal data?

The data controller of your personal data is Wallester AS, a company established under the laws of Estonia, registry code 11812882, address F. R. Kreutzwaldi 4, 10120, Tallinn, Estonia.

In case you have inquiries, requests or complaints regarding the processing of your personal data, you may forward them to at dpo@wallester.com.

In case you have complaints regarding the processing of your personal data, you may file them with the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) or the Data Protection Authority of the state in which you have permanent residence.