Privacy Notice

1. Introduction

The Privacy Notice describes how we collect, process, use and disclose your information, including any personal data we collect from you, or which you provide to us through the website https://payean.com/ (hereinafter referred to as the Website).

When you contact us via the Website, complete any forms or submit any details using the Website, we will collect, use and disclose your personal information as described in this Privacy Notice.

2. What is personal data?

Personal information includes any factual or subjective information, recorded or not, about an identifiable individual. In this policy definitions “personal data” and “personal information” shall be user interchangeably.

The General Data Protection Regulation (GDPR) (EU Regulation 2016/679) defines personal data as «any information relating to an identified or identifiable natural person (data subject), directly or indirectly, by reference to an identifier, such as name, an identification number, location data, an online identifier». Simply put, personal information is any information about you that enables your identification. The personal data we collect and use is described in this Privacy Notice.

3. Details of the Data Controller and the Data Protection Officer

The Data Controller is the company that determines the purpose and means of personal data processing: PAYEAN UAB, registration number 306061130, registered at Gedimino Ave. 44A-201, Vilnius, LT-01110, Lithuania.

4. Personal data we collect and process

We process certain personal data as described below:

1. When undergoing the Verification in order to gain the full access to the Services, the Customer shall provide the following data to the Administrator:
    - Name;
    - Surname;
    - Address;
    - Email address;
    - An image of a valid ID document issued by an authorized state body, containing a unique identification number and the Customer’s photo;
    - Mobile phone number.
      The Internal Policies may require the Customer to disclose information on source of wealth etc.
      To identify the Customer and manage fraud, the Administrator may demand that the Customer undergoes authentication with the use of videoconference, facial image data, such as photos of the face (including selfie images), a photo or scan of the face on the identification document, video screenshots and sound recordings.
2. When you communicate with us:

- Your contact email;
- Content of your communication, messages, and files you attach to your messages;
- Unique ticket system identifier;
- Technical data related to your messages (including date, time zone, environment, etc.).

3. Transaction information:
    - Transaction performed, including date, time, amount, currencies, technical usage data, and geolocation information;
    - Bank card details, such as cardholder name, expiry date, first 6 and last 4 digits of the card number;
    - Crypto wallet address.
4. Information from your device:
    - IP address;
    - Environment;
    - Log-in information;
    - Browser type and settings;
    - Time zone;
    - Operating system;
    - Type of device you use;
    - Unique device identifier;
    - Screen size;
    - Mobile network information;
    - Mobile operating system;
    - Type of mobile browser you are using;
    - Date;
    - Time and length of your visit.
5. Information we may receive from third parties:
    - Information received by one of our affiliates;
    - Information from payment systems, payment providers;
    - Information received by the card schemes (e.g. Visa, Mastercard, Unionpay, etc.), fraud prevention agencies, credit reference agencies, government and law enforcement agencies;
    - Information received via public sources like company registers, websites for enhanced due diligence checks.

5. Legal basis and use of your personal data

We only process your personal data where a lawful basis exists. The legal basis for each processing will be one of the following:

- Performance of a contract we enter with you;
- Our legal obligation;
- Our legitimate interests, taking into consideration your rights, interests, and expectations;
- Your consent.
- Performance of a contract we enter with you
  We process your personal data to provide you with the Services based on the Terms and Conditions that you accept when you use the System.
  We use your data to process transactions you make on the Website.
  We may send you important information about the system, suspicious transactions notifications, as well as provide technical support.
  We process personal data to assist you in resolving issues related to the use of System, when you contact Customers Support via ticket on the Website.
- Our legal obligation
  We process your personal data to comply with our legal obligations, in particular the requirements of anti-money laundering and terrorist financing legislation, to verify and confirm your identity as part of the KYC procedure.
  When you use the Services, we may send your data to the providers of these Services to meet AML requirements and follow KYC rules and “Travel Rule” obligations.
  We may use your data to assist any law enforcement authority with their investigation or disclose data required by a court order as we may be obliged to by law.
- Our legitimate interests
  We may use anonymized and aggregated data to analyse how Customers use our Services and evaluate the quality and convenience of our product, site operation and functionality.
  Likewise, we may also use your data to notify you about changes to our policies or new features.
  We take a risk-based approach to assess users and the transactions they make, as well as to detect and prevent fraudulent and other illegal activities. We collect, use, and store personal data for these purposes.
  When you contact Customer Care, we keep a record of the conversation. We do this to improve the quality of Services and products, protect our interests in case of disputes, evaluate the quality of the work of the employees, and train them.
- Your consent
  You may opt in to receive emails about Services, and allow us to measure the performance of marketing emails and analyse product use. You may withdraw your consent at any time.
  We may ask you to go through the liveness test to make sure that you are a living person and the documents submitted really belong to you. To achieve this, you will need to turn on the camera and turn your head so that the neural network can analyse the individual features of your face. Such analysis constitutes the processing of a special category of personal data, and can only be carried out based on your consent. The data collection

and processing are carried out by a third party, acting as a data processor on our behalf. You can read more about this in the “Disclosure of personal data to third parties” section.

2. Cookies

For information on what cookies are and how we use them, please refer to our Cookies Policy.

3. Automated decision-making

We use an automated risk assessment system to analyse ongoing transactions to prevent illegal and fraudulent activities. However, any significant decisions that may impact you will be taken by our employees based on a manual review.

4. How we keep your data secure

We are committed to making sure that your personal data is protected. We implement a variety of security measures to maintain the safety of your personal data when you enter it on the site or otherwise provide it to us.
Furthermore, we use data encryption techniques and authentication procedures to prevent unauthorized access to our systems and your data. Only authorized employees are granted physical access to the premises where data is processed and stored. The premises are being watched.
All supplied sensitive information is transmitted via Secure Socket Layer (SSL) technology. Card payment information encryption is compliant to PCI DSS. We authorize access to your personal data only for those employees who need it based on their job requirements (for example, customer support staff). All employees who access personal data are bound by a non-disclosure agreement. We implement continual training for our employees in regard to ensuring the security and confidentiality of personal data.
Personal data of the users being subjects to GDPR shall be processed only on the servers physically located within the European Union. We continuously improve our security procedures to ensure that we are in line with the best industry standards, thus ensuring a high level of protection of your personal data.

5. How long we keep your data

Your personal data will be retained by us for as long as necessary for the specific purpose for which it was collected, unless a longer retention is required by law. Information collected under AML laws requirements shall be kept for 8 years after the date of the last transaction. When your personal data is no longer needed and/or the term prescribed by law expires, we securely delete your data.

6. Disclosure of personal data to third parties

To provide Services, we may be required to share your data with third parties, such as:

To whom we may share your data?	Why do we share it?	Third-party name
Financial and banking institutions, such as bank card issuers and bank card acquirers, payment networks, including Visa and Mastercard.	To perform payment transactions, you may initiate using our network and your bank card and/or your bank account. Depending on the type of payment chosen by the Customer, payer or buyer, we will share the information with the	May vary depending on the payment method, region and requested service.

	financial institutions that validate and process each means of payment for corresponding approval, validation, and settlement.	
Third-party analytics providers.	To collect metrics and information regarding your use of our website, including evaluating how Customers use Services («Usage Data»), to develop new features, improve existing features or inform sales and marketing strategies, based on our legitimate interest to improve the Services. When we process Usage Data, any personal information is anonymized. The Website uses cookies and other tracking technologies to measure performance and collect metrics. We use GTM pixels to analyse how users interact with the Website and measure the effectiveness of our newsletters. You may find more information about the cookies we use in our Cookies Policy.	Google Inc., 1600 Amphitheatre Parkway Mountain View, CA 94043, USA ("Google"). Our website uses Google Analytics. On the Website, IP anonymization is enabled. For more information, you may read Google Privacy policy.
AML analytics and KYC service providers.	Fulfilment of our legal obligations under AML laws and fraud prevention monitoring.	Sum and Substance Ltd, 30 St. Mary Axe, London, England, EC3A 8BF ("Sum&Substance") - a verification and KYC service provider. For more information, you may read Sumsub Privacy notice.
Third-party ticket-system providers.	To facilitate our Customer Care service, and group the related requests, we use a ticket service. The ticket-system service provider does not have access to the content of your emails and is contractually bound to maintain the security and integrity of the processed data.	Zendesk International Ltd., 55 Charlemont Place, Saint Kevin's, Dublin, D02 F985 Ireland ("Zendesk") - a ticket system provider. When you submit a query to Payean via the ticket system, a unique identifier is assigned to you and an account with Zendesk is created. For more information, you may read Zendesk Privacy policy.
Email delivery service providers and online-based survey services providers.	We may send you special offers and news you may be interested in. Also, we may ask you to share your experience with Services, so we can improve them.	ECOMZ HOLDING LIMITED, 6B Georgiou Karyou, office 6B, Dasoupoli, Strovolos, Nicosia, Cyprus ("Unisender") - a marketing email delivery service provider. Unisender

		may apply technologies allowing to track when you receive and open email sent by us. You may opt out from receiving emails by clicking unsubscribe button in the email. For more information, you may read Unisender Privacy notice.
Other business partners, suppliers (including but not limited to IT suppliers, etc.) and affiliates.	To perform the contract we concluded in your interests, maintain the operation of the Services, fulfil our obligations.	Determined on a case-by-case basis and may vary depending on your region.
To prospective buyers of business.	If we buy, sell or transfer in other way any business or assets or in case of an actual or potential merger or similar business combination event, we may share your data to the new data controller. The basis for this processing is legitimate interest. In such cases, sharing personal data is required to facilitate the transaction.	Determined on a case-by-case basis.
To third parties such as courts, law enforcement or governmental authorities, or authorized third parties as required and permitted by law if such disclosure is reasonably necessary.	We may disclose your information to comply with our legal obligations, to respond to requests relating to criminal investigation, alleged or suspected illegal activities, or any other activities that may expose us or other users to legal liabilities, as well as to enforce our site policies and protect our or others' rights, property or safety.	Determined on a case-by-case basis.

Certain partners and service providers may change. This section shall be updated in a timely manner if such update is possible and reasonable.

7. Links to other websites

The Website may contain links to third-party websites. These third-party websites have separate and independent terms of use and privacy policies. Please refer to their policies before submitting any personal data to these websites. Therefore, we have no responsibility or liability for the content and activities of these websites.

8. Cross border transfer of data

Some of our partners and employees may be located outside the European Economic Area (EEA), so we may transfer data to the third countries. Such a transfer may only take place if appropriate guarantees

are in place to ensure an adequate level of protection of the rights of the personal data subjects. Our partners and providers are required to provide an adequate level of data protection in accordance with the terms of the contract we enter into with them.

9. Data subject rights

You have the right to exercise control over the way in which your personal data is processed:

Right to be informed. You are entitled to know how and why we process personal data. Therefore, we publish this Privacy Notice and are always ready to answer any of your questions.

Right of access. You can ask us to confirm whether we are processing your personal data. You can ask for detailed information about how we collect, process, use, store and share your data.

Right to rectification. We strive to maintain the integrity of the data we store and keep it up to date. Therefore, you can always ask us to clarify and correct outdated or inaccurate information.

Right to erasure. You may request to delete your personal data. You may file a request by creating a ticket in the Customer support chat available on the Website. Bear in mind that we are required by law to store some of your personal data, so we can't remove all of your info from the system. The right to erasure will not apply to such processing. But we'll delete information that's no longer needed.

Restrict and object to processing. You have the right to restrict or object to the processing of your personal data.

Right to data portability. You may ask us to transfer your data to another entity providing similar services, if it is technically possible to do so and unless it is not restricted by law. The data will be transmitted in a structured, commonly used and machine-readable format.

Right to withdraw consent. Where we have specifically requested your consent to process your personal data, you have the right to withdraw your consent at any time by filing a request by creating a ticket in the Customer support chat available on the Website specifying which consent you are withdrawing. You can opt out of receiving materials from us electronically by clicking the «unsubscribe» link in any e-mail communications we might send you.

Right to complain. You may lodge a complaint if you feel like your rights have been violated. Please refer to Section 14 for further details. 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.

You may exercise your rights described above by sending a request by creating a ticket in the Customer support chat available on the Website. Before we provide you with any confidential information, we must ensure that you are indeed the person you claim to be.

We will provide you with the requested data free of charge. However, if the requests are manifestly unfounded or excessive, in particular because of their repetitive character, we may charge a reasonable fee considering the administrative costs of providing the information or communication or taking the action requested.
Kindly note that there may be legal reasons when we will not be able to fulfil your request.

10. Filing a complaint

If you believe that your rights have been violated, you may file a complaint to the supervisory authority in Lithuania or your country of residence or place of the alleged violation. If you are in the EU, you can find the relevant supervisory authority on the European Data Protection Board website.

11. Changes to our Privacy Notice

Any changes we make to our Privacy Notice in the future will be posted directly on this page and, where appropriate, notified to you by e-mail.

12. Contact

Questions, comments and requests regarding our Privacy Notice are welcomed and should be addressed to our Data protection officer to the email address privacy@payean.eu.