Visa Payment Card Privacy Policy

Contis Financial Services Limited or Finansinės paslaugos “Contis“, UAB (“we”, “us”, or “our”) is committed to protecting and respecting your privacy.

This policy together with the Visa Payment Card Account Terms and Conditions and any other documents referred to in them, sets out the basis on which any personal data we collect from you, or that we collect about you, on the Paysera website ("Website"), on the Paysera app ("App"), or when you communicate with us by email, telephone, or post will be processed by us.
We will be the data controller of your personal data which you provide to us or which is collected by us about you. This means that we are responsible for deciding how we hold and use personal data about you and that we are required to notify you of the information contained in this policy. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it. The terms and conditions of your account will identify which Contis company is the controller of your personal data.

We may be provided with this data by a client of ours Paysera LT, UAB who provides the Website or App for the purposes of applying for the account and providing some account services. Paysera LT, UAB is an independent data controller and will also be acting as a processor of ours. For further information as to the type of personal data we share with the client and the uses made by them of that data see the data sharing section of this Policy below. You should also read the client Privacy Policy which is available on the Website or App.

If you have any queries, you can contact us using the details provided at the end of this Policy in the “Contacting us” section.

Ensuring the lawful use of your personal data

We will only use your personal data where we have a lawful basis to do so. We will usually only use your data:

1. where it is necessary for us to enter into and/or perform a contract with you (for example, to create your account and provide our services to you);
2. in a way which might reasonably be expected as part of running our business and which does not materially impact your interests, rights, or freedoms. For example, we might collect technical information about you when you visit our Website or App to improve your experience on our Website or App. Please contact us using the details below if you would like further information about this;
3. to comply with our legal obligations. For example, to pass on details of people who are involved in fraud and to carry out anti-money laundering checks;
4. in some cases, where you have consented to us using your data, for example, where you subscribe to our email newsletter.

Further details of how we will use your personal data are provided below.

What information we collect from you and how we use it

When you apply to create an account

When you apply to create an account on the Website or App, we will need to collect some or all of the following details about you:

- Name
- Residential addresses (current and previous)
- Business name
- Business address
- Date of birth
- Gender
- Email address
- Telephone numbers
- ID document numbers such as passport, driving licence, or ID card
- Image or photo of you

We will use this information for the purposes of processing your application and, if your application is successful, creating and managing your account and providing any products or services you request to you. If you have consented, we will also send our newsletter to you by email.

You will not be able to apply to create an account or order products or services from us without providing this information.

This information may be provided to us by the client, we will become data controller of this information once we receive it from them.

Fraud and money laundering checks

In order to process your application and before we fulfil your order and provide services, goods, or financing to you, we will use the information you provided to create your account to undertake checks for the purposes of preventing fraud and money laundering, and we may need to verify your identity. This may involve sharing your personal data with fraud prevention agencies. We will continue to carry out these checks on a regular basis while you are a customer of ours.

When we and fraud prevention agencies process your personal data, we do so on the basis that we have a legitimate interest in preventing fraud and money laundering, and to verify identity, in order to protect our business and to comply with laws that apply to us. Such processing is also a contractual requirement of the services or financing you have requested.

We and fraud prevention agencies may also enable law enforcement agencies to access and use your personal data to detect, investigate, and prevent crime.

Fraud prevention agencies can hold your personal data for different periods of time, and if you are considered to pose a fraud or money laundering risk, your data can be held for up to six years.

Automated decisions

As part of the processing of your personal data, decisions may be made by automated means. This means we may automatically decide that you pose a fraud or money laundering risk if:

- our processing reveals your behaviour to be consistent with that of known fraudsters or money launderers; or is inconsistent with your previous submissions; or
- you appear to have deliberately hidden your true identity.

You have rights in relation to automated decision making: if you want to know more please contact us using the details below.

Consequences of processing

If we or a fraud prevention agency determine that you pose a fraud or money laundering risk, we may refuse to provide the services and financing you have requested or we may stop providing existing services to you.

A record of any fraud or money laundering risk will be retained by the fraud prevention agencies and may result in others refusing to provide services, financing, or employment to you. If you have any questions about this, please contact us on the details below.

Other than the automated processing set out above, we shall not carry out solely automated decision-making using your personal data.

When you contact us

When you contact us, we will need to collect personal data about you to verify your identity before we disclose any information to you for data security purposes. We will be unable to deal with your query unless you provide the information we request. We may also collect any other personal data you choose to provide to us when communicating with us. We will only use that personal data for the purposes of dealing with your enquiry.

The means, purpose, and legal basis for data processing

We use your personal data for various purposes related to your use of the account and services. We will process your data where we have a lawful basis to do so. We will usually only use your data:

1. where it is necessary for us to enter into and/or perform a contract with you. For example, to create your account and provide payment services to you;
2. in a way which might reasonably be expected as part of running our business and which does not materially impact your interests, rights, or freedoms. For example, to improve how we manage and process your payments;
3. to comply with our legal obligations. For example, to pass on details of people who are involved in fraud and to carry out anti-money laundering checks.

We use your personal data for the following purposes:

- to create and manage your account with us;
- to process payment transactions from and to your account;
- to carry out the required checks on your identity and monitor your use of your account to check for fraud;
- to facilitate your use of your account;
- to communicate with you and provide you with customer support;
- to share information with our suppliers and other third parties (such as banking institutions, payment facilitators, and card operators) where required.

The table below sets out further information about the purposes for which we use data about you, with the corresponding methods of collection and legal basis that we rely upon for its use.

PURPOSE	LAWFUL BASIS FOR PROCESSING
Creating and managing your account • to apply for and create your account • to administer and manage your account • to retain your account profile information	To fulfil our contractual obligations to you in providing the account and services. Our legitimate interests in operating and improving our services to you. Our legal obligations to comply with regulations that apply to us.
Carrying out identification and fraud checks • to carry out the required checks on your identity and enable you to use your account and card	To fulfil our contractual obligations to you in providing the account and services correctly. Our legitimate interests in operating and improving our services to you and how we deal with financial crime. Our legal obligations to comply with regulations that apply to us.

Facilitating your use of your account and card

- to administer your financial transactions (e.g., payments, refunds, cashback, transfers, etc.)
- to provide details of your transactions
- to retain records of your transactions and spending activities

To fulfil our contractual obligations to you in providing the account and services.

Our legitimate interests in operating and improving our services to you.

Our legal obligations to comply with regulations that apply to us.

Monitoring your use of the account and card to detect fraudulent behaviour

- to detect and prevent financial crime
- to satisfy our legal and regulatory obligations
- to manage risk for us, you, and our other users

To fulfil our contractual obligations to you in providing the account and services correctly.

Our legitimate interests in operating and improving our services to you and how we deal with financial crime.

Our legal obligations to comply with regulations that apply to us.

Communicating with you and providing you with customer support

- to investigate your complaint or query
- to provide you important information or inform about changes to your terms and conditions

To fulfil our contractual obligations to you in providing the account and services.

Our legitimate interests in operating and improving our services to you.

Our legal obligations to comply with regulations that apply to us.

Sharing data with our suppliers and other third parties (such as banking institutions, payment facilitators, and card operators) where required

- see the *Disclosures of your information* section for more information

To fulfil our contractual obligations to you in providing the account and services.

Our legitimate interests in operating and improving our services to you.

Our legal obligations to comply with regulations that apply to us.

Sharing data with Paysera LT, UAB in order for Paysera LT, UAB to:

- administer, manage, and provide the Paysera LT app and website, manage their relationship with you, and deliver relevant content to you
- analyse and develop other products and services
- provide customer support to you regarding the account, card, and payments

To fulfil our contractual obligations to you in providing the account and services.

Our legitimate interests in operating and improving our services to you.

Our legal obligations to comply with regulations that apply to us.

The information we receive from other sources

We are also working closely with third parties (including, for example identity verification agencies, marketing agencies, and fraud prevention agencies) and we may receive information about you from them for the purposes of identity verification, marketing, and fraud prevention.

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that the reason is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will usually notify you and explain the legal basis which allows us to do so.

Disclosures of your information

We will disclose your information to:

- Fraud prevention agencies, identity verification services, and other organisations for the purposes of preventing fraud and money laundering. For example, we share your personal data with CIFAS when we carry out our fraud prevention and anti-money laundering checks and if we suspect that you have committed fraudulent activity;
- Our group companies, for the purposes of processing transactions and providing services relating to your account;
- Third party service providers and agents, such as:
    - IT companies, e.g. SherWeb who provide data hosting services;
    - telephony companies, e.g. Talkdesk who provide our telephone systems;
    - payment schemes, e.g. Visa who are our card payment provider;
    - card manufacturers, e.g. TAG who are one of our approved card manufacturers;
    - auditors, e.g. ECSC who audit our compliance to PCIDSS standards;
    - distributors and agents of ours who market and provide services to you for the account and card
- in order to allow us to manage our business and to provide the products and services to you;

- In the event that we sell or buy any business or assets, to the prospective seller or buyer of such business or assets;
- If Contis Financial Services, or Finansinės paslaugos "Contis“, UAB, or substantially all of its respective assets are acquired by a third party, to the acquiring third party; or
- A third party if we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to enforce or apply our Terms and Conditions and other agreements; or to protect the rights, property, or safety of Contis Financial Services Limited, Finansinės paslaugos "Contis", UAB, our customers or others.

Protecting your information

Your data is secured by encryption, firewalls, and Secure Socket Layer (SSL) technology. This is industry standard encryption technology which manages the security of messages transmitted across the internet. When we receive your data, we store it on secure servers which can only be accessed by us. We store your passwords using one way encryption which means we do not know what your password is.

Storing your data within and outside the EEA

Our third-party data host provider uses servers located in the UK and Europe to store personal data. As a result, when you use the Website or App to make transactions or update your account information, your personal data may be transferred to the UK which is located outside of the European Economic Area and so is not governed by European data protection laws.

However, Finansinės paslaugos "Contis", UAB has entered into EU standard contractual clauses with any third party or group company in order to safeguard personal data which is processed or stored in the UK. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this policy when it is transferred, stored, or processed in this way.

Whenever fraud prevention agencies transfer your personal data outside of the European Economic Area, they impose the EU standard contractual clauses adopted by the European Commission on the recipients of that data in order to safeguard personal data when it is accessed from outside of the European Economic Area. They may

also require the recipient to subscribe to international frameworks intended to enable secure data sharing.

More information about the EU Standard Contractual Clauses is available here.

Future changes

Any changes we make to our policy will be put on our Website and App and, where appropriate, introduced to you by e-mail. Please check for updates from time to time.

Retention of your data

We will retain your personal data for as long as you continue to use our services. Thereafter, we may retain your information for an additional period as is permitted or required under applicable laws. For example:

- If you hold an account with us, your personal data will be retained for eight years after the closure of your account to comply with our obligations under anti-money laundering regulations;
- If you make a complaint, your personal data relating to that complaint will be retained for five years from the resolution of that complaint to defend against legal claims; and
- If you make any transactions on your account, your personal data relating to that transaction will be retained for seven years from the date of the transaction to comply with taxation and accountancy legislation.

Your rights

Data protection laws provide you with the following rights to:

- request access to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it;
- request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected;
- request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below);
- request the restriction of processing of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it; and
- request a copy of your personal data which you have provided to us, in a structured, commonly used, and machine-readable format and the right to transfer it, or to require us to transfer it directly, to another controller;
- object to the processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal data for direct marketing purposes.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights above). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

If you are unhappy about how your personal data has been used please refer to our complaints procedures which is available by contacting us. You also have a right to complain to the supervisory authority, which in the United Kingdom is the **Information Commissioner's Office** and in Lithuania – **the State Data Protection Inspectorate**, who regulate the processing of personal data.

Contacting us

If you have any questions about this policy, you can contact us by using the ‘Contact us’ facility on the Website or App or in the following ways:

By post at:
Data Protection Officer
Contis
Navigation House
Belmont Wharf
Skipton
North Yorkshire
BD23 1RL

By email at: dpo@contis.com