Updated: 05/10/2026

Contis Privacy Policy

UAB „Finansinės paslaugos „Contis“ (“Contis”, “we”, “us” or “our”) is a Lithuanian electronic money institution, registered in the Register of Legal Entities of the Republic of Lithuania under company code 304406236, with its registered office at Pilaitės pr. 16, LT-04352 Vilnius, Lithuania. Contis holds Electronic Money Institution Licence No. 53, issued by the Bank of Lithuania on 23 July 2019 (authorisation code LB001896), and is supervised by the Bank of Lithuania. Contis is a member of the Paysera Group and acts as the controller of your personal data for the processing activities described in this Privacy Policy.

This policy, together with our Terms and Conditions for your account and any other documents referred to in them, sets out the basis on which any personal data will be processed by us. We may collect personal data from you on any Websites or Apps we previously provided, or when you communicate with us by email, telephone or post.

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.

Your personal data may have been provided to us by a distributor who operated the website or app through which you applied for your account. That distributor may have acted as an independent data controller and also as a processor on our behalf. The distributor relationship has now ended and we no longer share personal data with the distributor. If you require information about how the distributor handled your personal data during that period, please refer to the distributor’s own privacy policy.

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 only use your data:

- 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).
- 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.
- 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.
- in limited cases, we may rely on your consent as a legal basis for processing – for example, if you have

explicitly consented to receiving information from us for a specific purpose not otherwise covered in this policy. Where we rely on consent, you have the right to withdraw it at any time (see below).

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 applied to create an account on the Website or App, we collected 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
- Copies of ID documents, such as passport, driving licence or ID card.
- Image or photo of you

We used this information for the purposes of processing your application and creating and managing your account and providing any products or services you request to you.

You will not have been able to apply for an account or order products or services from us without providing the mandatory elements of this information, which was requested as part of your specific account application.

Some of this information may have been provided to us by the distributor at the time your account was opened. We became the data controller of that information upon receipt.

Special categories of personal data

We do not intentionally collect special categories of personal data about you (such as data relating to your racial or ethnic origin, political opinions, religious beliefs, health, or biometric data). However, information that could be inferred as falling within these categories may occasionally be apparent from transaction data we hold – for example, payments to healthcare providers or places of worship.

Where transaction data incidentally reveals or allows inferences about special categories of personal data, we do not seek to classify individuals on the basis of such information. We process such data only where and to the extent permitted by applicable law, including where necessary to comply with our legal obligations or to establish, exercise or defend legal claims, and subject to appropriate safeguards.

If we ever need to process special category data for a purpose not covered above, we will seek your explicit consent at that time.

Fraud and money laundering checks

When you applied for your account, we used the information you provided to carry out checks to prevent fraud

and money laundering, and to verify your identity. This involved sharing your personal data with fraud prevention authorities. Even though your account is now closed, we may continue to carry out checks using the data we hold as required by law.

When we and fraud prevention authorities process your personal data, we do so because such processing is necessary for compliance with legal obligations to which we are subject. We and fraud prevention authorities also have a legitimate interest in preventing fraud and money laundering, verifying identity, protecting our business and preventing financial crime. Such processing is also a contractual requirement of the services or financing you have requested.

Processing of personal data relating to actual or suspected criminal offences, including fraud and money laundering risk assessments, is carried out under Article 10 GDPR.

Such processing is authorised by Lithuanian law, specifically the Law on the Prevention of Money Laundering and Terrorist Financing, which confers authority on regulated payment institutions to carry out such processing for the purposes of preventing financial crime.

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

Fraud prevention and identity verification service providers retain personal data in accordance with their applicable legal obligations and retention policies.

Automated decisions

We use automated systems to identify, assess and prioritise potentially suspicious or fraudulent activity. These systems may generate alerts or risk indicators, but do not by themselves make decisions that produce legal or similarly significant effects. Any such final decision is subject to appropriate human review.

Where such a decision has a significant effect on you, you have the right to:

(i) ask for human review – a member of our staff who has the authority to change the decision will review it carefully, taking into account anything you tell us;

(ii) have your say – you can give us information about your situation before or during that review; and

(iii) challenge the outcome – you can ask us to look at it again from scratch.

To exercise any of these rights, please contact us using the details in the “Contacting us” section.

Consequences of processing

If we, or a fraud prevention authority, 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.

Information relating to identified fraud or money laundering risk may affect decisions made by other financial service providers where such information is lawfully shared with them. If you have any questions about this, please contact us on the details below.

Other than the automated processing set out above, we will not make any decisions about you based entirely on automated processing.

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 legal basis for this processing is our legitimate interests (Article 6(1)(f) GDPR) in verifying your identity for security purposes and in responding to your enquiry effectively.

Reminders to claim funds on closed accounts

If your account has been closed and funds remain held on your behalf, we will use the contact details we hold for you to send you reminders to claim those funds. We do this on the basis of our legitimate interests in ensuring that funds are returned to their rightful owner, and to comply with our obligations as a regulated payment institution under applicable payment services legislation.

We will not use your contact details for any other communications. If you no longer wish to receive fund reminders, please contact us using the details in the “Contacting us” section below and we will discuss the options available to you, including returning your funds by alternative means.

How we use data about you, for what purpose and legal basis

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

- 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.
- where it is necessary for the purposes of our legitimate interests or those of a third party, provided that those interests are not overridden by your interests, rights and freedoms. These legitimate interests include preventing fraud and financial crime, managing and mitigating operational and legal risks, improving the security and integrity of our systems, and fulfilling our obligations as a regulated payment institution. For example, to improve how we manage and process your payments.
- 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; and
- 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.

Creating and managing your account	**Contract (Art. 6(1)(b)); Legal obligation (Art. 6(1)(c)); Legitimate interests (Art. 6(1)(f)): operating our services**
Carrying out identity and fraud checks	**Legal obligation (Art. 6(1)(c)); Legitimate interests (Art. 6(1)(f)): preventing financial crime**
Facilitating use of account (transactions, refunds, transfers)	**Contract (Art. 6(1)(b)); Legal obligation (Art. 6(1)(c))**
Monitoring account use to detect fraud	**Legal obligation (Art. 6(1)(c)); Legitimate interests (Art. 6(1)(f)): preventing financial crime**
Communicating with you and providing customer support	**Contract (Art. 6(1)(b)); Legitimate interests (Art. 6(1)(f)): resolving queries**

Sharing data with third-party suppliers and card operators

Contract (Art. 6(1)(b)); Legal obligation (Art. 6(1)(c)); Legitimate interests (Art. 6(1)(f)): operating our payment services

The information we receive from other sources

We also receive information about you from third parties, including identity verification service providers and fraud prevention authorities, for the purposes of verifying your identity and preventing fraud and money laundering.

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 reason is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so before any such processing begins.

Disclosures of your information

We will disclose your information to:

- Fraud prevention authorities, identity verification services and other organisations for the purposes of preventing fraud and money laundering. For example, we share your personal data with fraud prevention authorities operating within the European Union 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;
    - payment schemes e.g. Visa who are our card payment provider;
    - auditors e.g. ECSC who audit our compliance with PCI DSS standards;
    - 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, we may disclose your personal data to the prospective seller or buyer of such business or assets. If UAB „Finansinės paslaugos „Contis“ or substantially all of its assets are acquired by a third party, personal data held by us may be transferred to the acquiring entity. Such disclosures are made on the basis of our legitimate interests (Article 6(1)(f) GDPR) in facilitating a lawful business transfer, and any acquiring entity will be required to use your personal data in accordance with this policy;

- 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 UAB „Finansinės paslaugos „Contis“, our customers or others.

Protecting your information

Your data is secured using appropriate technical and organisational measures, including encryption, firewalls, and Secure Socket Layer (SSL) technology. We control access to personal data on a need-to-know basis, and our staff receive training on data protection obligations. We store your passwords using one-way encryption. When we receive your data, we store it on secure servers accessible only to authorised personnel.

Personal data breaches

We will notify the State Data Protection Inspectorate or another competent supervisory authority of a personal data breach without undue delay and, where feasible, not later than 72 hours after becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Closed accounts – funds still held

If your account has been closed but funds remain held by us on your behalf, we continue to process your personal data. The purposes and legal bases for this continued processing are as follows:

- To identify you as the rightful owner of the funds and to facilitate their return to you: this processing is carried out on the basis of legal obligation (Article 6(1)(c) GDPR), arising from our obligations as a licensed electronic money institution under applicable Lithuanian and EU payment services and electronic money legislation.
- To comply with anti-money laundering, counter-terrorist financing, and regulatory reporting obligations: legal obligation (Article 6(1)(c) GDPR).
- To maintain transaction and accounting records as required by law: legal obligation (Article 6(1)(c) GDPR).
- You cannot access your account while it is closed. However, you may contact us using the details in the “Contacting us” section to request information about your funds and the process for their return to you.

While funds remain held in your name, certain data protection rights are restricted:

- Some of your data protection rights may not apply, or may apply only to a limited extent, where Contis is required to continue processing particular personal data to identify the person entitled to the funds, return the funds, comply with legal or regulatory obligations, maintain statutory records or establish, exercise or defend legal claims. Each request will be assessed individually, and we will explain the applicable legal basis where we are unable to comply with it in full.
- Right to data portability: this right is restricted to the extent that the relevant data relates to the safeguarding of your funds.

Once your funds have been returned, your personal data will be retained only as required by applicable law (see “Retention of your data” below).

Storing your data within and outside the European Economic Area (EEA)

Personal data may be transferred to the United Kingdom. The European Commission has determined that the United Kingdom ensures an adequate level of protection for personal data under Article 45 of the EU General Data Protection Regulation. This is reflected in Commission Implementing Decision (EU) 2025/2574 of 19 December 2025, which applies until 27 December 2031, unless extended. Transfers to the United Kingdom may therefore be made on the basis of that adequacy decision and do not require additional transfer safeguards, such as the European Commission's standard contractual clauses.

For transfers of personal data to countries outside the European Economic Area other than the United Kingdom, UAB „Finansinės paslaugos „Contis" uses the Standard Contractual Clauses (legal agreements approved by the European Commission) adopted on 4 June 2021 (Commission Implementing Decision 2021/914). Before making such transfers, we carry out an assessment of transfer risks to evaluate the specific transfer and implement any additional measures required.

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.

Further information about the 2021 EU Standard Contractual Clauses is available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D0914.

Future changes

Any material changes to this policy – in particular, changes to the purposes for which we use your personal data, the legal bases we rely on, or your data protection rights – will be notified to you by email before they take effect. For minor or administrative changes that do not affect your rights, we will update this policy and note the revision date at the top of the document.

Retention of your data

As your account is now closed, we retain your personal data only for as long as is necessary to fulfil the purposes set out in this policy and for as long as required by applicable law. The specific retention periods that apply are set out below.

- Your personal data will be retained for up to eight years from the date of closure of your account, to comply with our obligations under anti-money laundering regulations (specifically Article 19 of the Law on the Prevention of Money Laundering and Terrorist Financing) and to allow us to defend legal claims during the applicable limitation period;
- 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.

Where funds remain held after account closure, personal data necessary to identify the person entitled to those funds, account for the funds and facilitate their return will be retained for as long as the funds remain outstanding and thereafter for the applicable statutory retention period. Other personal data remains subject to the retention period applicable to the relevant category of data. Where your account has been closed but funds

remain held on your behalf by us, only the retention period applicable to personal data processed for identifying the person entitled to the funds, accounting for the funds and facilitating their return runs from the date on which the funds are returned. All other personal data remains subject to the retention periods applicable to the relevant processing purpose.

Your rights

Data protection laws provide you with the following rights to:

- request access to your personal data (commonly known as a ‘subject access request’ (SAR)). 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 that we delete your personal data. Because your account is closed and banking, anti-money laundering and tax laws require us to keep our records, we will not be able to delete most of your data. We will always explain what we are keeping and why;
- 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;
- request a copy of the personal data you provided to us in a structured, commonly used, and machine-readable format, and the right to have it transferred to another controller – where technically feasible. Note that this right applies only to data that was processed on the basis of your consent or on the basis of a contract with you, and only where the processing is carried out by automated means. It does not apply to personal data we are required to retain solely by law; and
- 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.

Your right to object

Where we rely on legitimate interests as the legal basis for processing your personal data, you have the right to object to that processing at any time on grounds relating to your particular situation. If you object, we will cease processing your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or where the processing is necessary for the establishment, exercise, or defence of legal claims.

We do not carry out direct marketing. The only communications we send are reminders to former account holders to claim funds remaining on their closed accounts. These communications are not marketing and are sent on the basis of our legitimate interests in ensuring funds are returned to their rightful owners.

To exercise your right to object, please contact us using the details in the “Contacting us” section below.

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, or refuse to comply, if your request is manifestly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

Where we rely on your consent as the legal basis for processing your personal data, you have the right to withdraw that consent at any time by contacting us using the details in the “Contacting us” section below. Withdrawing your consent will not affect the lawfulness of any processing we carried out before you withdrew it. Following withdrawal, we will cease processing your personal data for that purpose, unless we have another legal reason on which to continue to do so.

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 are available by contacting us. You also have a right to complain to the supervisory authority. The supervisory authority for UAB „Finansinės paslaugos „Contis“ is the State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija) in Lithuania: https://vdai.lrv.lt/en/. If you are located in another EU member state, you may also lodge a complaint with the supervisory authority of that member state.

Contacting us

We have appointed a Data Protection Officer (DPO) in accordance with Article 37 of the GDPR. Our DPO is responsible for overseeing compliance with this policy and with applicable data protection law. If you have any questions about this policy or about how we process your personal data, please contact our DPO using the details below.

If you have any questions about this policy, you can contact us:

By post at:

Data Protection Officer

UAB „Finansinės paslaugos „Contis“

Pilaitės pr. 16, Vilnius, LT-04352, Lithuania

By email at: dpo@contis.com

Agreement History

Contis Privacy Policy agreement version before 05.10.2026