Updated: October 5, 2026

Monavate onChain Privacy Policy

EU/EEA Version

This Privacy Policy explains how Monavate Ireland Limited, trading as Monavate onChain ("Monavate onChain," "we," "our," or "us"), collects, uses, shares, and protects your personal data when you use the Monavate onChain Custodial Card and associated Services, in accordance with Regulation (EU) 2016/679 (the "General Data Protection Regulation" or "GDPR"). This Policy applies to residents of the European Economic Area. Any capitalized terms not defined herein have the meaning set forth in the Monavate onChain Custodial Card Terms and Conditions described in Section 2.1 herein.

1. Who We Are

1.1. Data Controller

Monavate Ireland Limited, a company incorporated in Ireland with registered number 741457 and registered office at Ground Floor, 71 Lower Baggot Street, Dublin, D02 P593, Ireland, is the data controller responsible for your personal data in connection with the Services described in this Policy.

1.2. Data Protection Contact

If you have any questions about this Policy or how we handle your personal data, you can contact our Data Protection Officer at dpo@monavateonchain.com.

2. Personal Data We Collect

2.1. Information You Provide

We collect personal data you provide directly, including your name, address, date of birth, national identification or tax reference number, telephone number, email address, and a copy of a government-issued photo identification document or other documentation bearing your photo, as described in Section 4.3 of our Monavate onChain Custodial Card Terms and Conditions ("Terms and Conditions"), which are available here.

2.2. Biometric Data

As part of our identity verification process, you may be asked to provide a selfie or short video, which our identity verification software provider uses to perform facial matching and liveness detection against your government-issued identification document. This constitutes special category data, specifically biometric data used for the purpose of uniquely identifying you, under Article 9 of the GDPR. We process this data only with your explicit consent, which you provide at the point of onboarding. You may withdraw this consent at any time, but doing so may mean we are unable to verify your identity or provide you with a Card.

2.3. Information We Collect Automatically

We collect certain information automatically when you use our mobile application or web platform, including device identifiers, IP address, log data, and information about how you interact with the Services.

2.4. Information From Third Parties

We may receive personal data about you from the Program Manager, the Bank, identity verification providers, fraud prevention services, and other third parties engaged in connection with the Card Program, as described in Section 4 below. This may include information about the originator or beneficiary of a transfer of Supported Assets, which the Program Manager or the Bank collects and shares with relevant parties as required by applicable anti-money laundering and transfer-of-funds laws and regulations.

2.5. Consequences of Not Providing Your Personal Data

Providing the personal data described in Section 2.1 is necessary for us to verify your identity and open a Card Account, as required by applicable anti-money laundering laws and regulations and as a condition of our contract with you by way of the Terms and Conditions. If you do not provide this information, we will not be able to open a Card Account for you or provide you with a Card.

3. How and Why We Use Your Personal Data

We only process your personal data where we have a valid legal basis to do so under the GDPR. Below, we set out the main purposes for which we process your personal data and the legal basis we rely on for each.

Onboarding and identity verification. We process your personal data to verify your identity, assess your eligibility for the Services, and comply with anti-money laundering and counter-terrorist financing law. Legal basis: compliance with a legal obligation; and performance of a contract with you.

Biometric identity verification. Where our identity verification process includes a selfie or liveness check, as described in Section 2.2, we process this special category data on the basis of your explicit consent under Article 9(2)(a) of the GDPR.

Providing and managing your Card Account. We process your personal data to operate your Card Account, provide customer service, and communicate with you about the Services. Legal basis: performance of a contract with you.

Fraud prevention and security. We process your personal data to detect, investigate, and prevent fraud, unauthorised transactions, and other security threats. Legal basis: legitimate interests, specifically our interest and that of our group companies, the Program Manager, and the Bank in protecting you, us, and our Services from fraud and financial crime; and compliance with a legal obligation.

Sharing within our corporate group for shared services. We process your personal data to enable shared services across our corporate group, including customer support, product development, commercial and marketing activities, risk management, and compliance functions, as described in Section 4.1 below. Legal basis: legitimate interests, specifically our interest and that of our Affiliates in operating efficiently and consistently as a group. We have assessed that this interest is not overridden by your rights and interests, taking into account that such sharing is limited to what is necessary for these purposes.

Improving our Services. We process your personal data to analyse how our Services are used and to improve them. Legal basis: legitimate interests, specifically our interest in understanding and improving our Services, balanced against your rights and interests.

Legal and regulatory compliance. We process your personal data where necessary to comply with applicable law, respond to requests from competent authorities, or establish, exercise, or defend legal claims. Legal basis: compliance with a legal obligation; and legitimate interests.

Marketing communications. With your consent, we may send you marketing communications about our Services, rewards programmes, and related offers. Legal basis: consent. You can withdraw your consent, or object to receiving marketing communications, at any time, as described in Section 7.

4. Who We Share Your Personal Data With

4.1. Our Corporate Group

We are part of a corporate group that includes Monavate onChain's parent, and affiliated companies controlled by or under common control with Monavate onChain (our "Affiliates"). We may share your personal data with any of our current Affiliates, and with any company that becomes our Affiliate in the future, for the purposes described in Section 3 above, including shared customer support, product development, commercial and marketing activities, risk management, and compliance functions. Where an Affiliate that receives your personal data is located outside the European Economic Area, such transfer will remain subject to the same appropriate safeguards, as described in Section 5 below.

4.2. The Program Manager and the Bank

We share your personal data with the Program Manager and the Bank to the extent necessary for them to provide the Services, including processing Card transactions, holding funds in your Card Account, and performing identity verification and anti-money laundering checks. The Program Manager's and the Bank's own use of your personal data is governed by the Program Manager Terms and the Bank's own disclosures, not by this Policy.

4.3. Other Service Providers

We may share your personal data with third parties that provide services on our behalf, such as hosting, information technology, customer support, identity verification software, including biometric liveness and facial matching verification, and fraud prevention, acting on our instructions and under contractual obligations consistent with the requirements set forth under the GDPR.

4.4. Legal and Regulatory Disclosures

We may disclose your personal data to competent authorities, law enforcement, or other third parties where we believe in good faith that disclosure is required by applicable law, or necessary to protect our rights, your safety, or the safety of others.

4.5. Business Transfers

If we are involved in a merger, acquisition, restructuring, or sale of assets, your personal data may be transferred as part of that transaction. We will notify you of any such transfer and any resulting change in how your personal data is handled.

4.6. Co-Branded Partners

You may access the Custodial Card through a Co-Branded Partner's application or platform. We do not share your personal data with a Co-Branded Partner in connection with your use of the Custodial Card. If a Co-Branded Partner separately collects your personal data in connection with its own products or services, that collection is governed by the Co-Branded Partner's own privacy practices, which are not addressed by this Policy.

5. International Data Transfers

Transfers of your personal data to the United Kingdom are covered by the European Commission's adequacy decision for the UK, and may take place without further safeguards. Where we transfer your personal data to any other country outside the European Economic Area, we will ensure that an appropriate safeguard is in place, such as an adequacy decision of the European Commission, Standard Contractual Clauses, or another legally recognised transfer mechanism, together with any supplementary measures necessary to ensure your personal data continues to receive a standard of protection comparable to that provided under the GDPR. You may request further information about the safeguards we use, including a copy of the relevant documentation, by contacting us as set out in Section 1.2.

6. How Long We Keep Your Personal Data

We retain your personal data for five (5) years following the end of our relationship with you, or for as long as otherwise necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

7. Your Rights

Under the GDPR, you have the right to:

- access the personal data we hold about you;
- request rectification of inaccurate personal data;
- request erasure of your personal data, subject to certain exceptions, including our legal obligation to retain certain records;
- request restriction of the processing of your personal data;
- object to processing based on legitimate interests;
- receive your personal data in a structured, commonly used, machine-readable format, and request that we transmit it to another controller, where technically feasible;
- withdraw your consent at any time, where processing is based on consent, without affecting the lawfulness of processing before withdrawal; and
- lodge a complaint with your national data protection supervisory authority.

You also have an absolute right to object to the processing of your personal data for direct marketing purposes, including any related profiling, at any time, free of charge, and without needing to give a reason. To do so, please contact us using the details in Section 1.2, or use the unsubscribe mechanism provided in our marketing communications.

To exercise any of these rights, please contact us using the details in Section 1.2. We will respond to your request within the timeframes required by the GDPR.

8. Automated Decision-Making

We use automated identity verification software and internal automated rules to screen and detect potential identity matches or mismatches, including against relevant sanctions, watchlists, and fraud-risk indicators, as part of onboarding and ongoing account monitoring. This screening may result in a delay, decline, or restriction of your Card Account pending further review. Where a potential match or inconsistency is identified, our customer support team may contact you to request additional or corrected information, which is then evaluated by our compliance team, who have the authority to resolve the matter. You have the right to express your point of view, request human intervention, and contest any decision made on this basis. To the extent this processing falls within the scope of Regulation (EU) 2024/1689 (the "EU AI Act"), we will comply with the applicable requirements of that Regulation. To request human intervention or contest any decision as described herein, please contact us using the details in Section 1.2.

9. Security Measures

We take appropriate technical and organisational measures to protect your personal data against loss, misuse, and unauthorised access. We do not store your full card number (PAN) or CVV. Where we reference your Card internally, we use a randomised Card ID assigned by the Issuer, which does not itself constitute sensitive cardholder data.

10. Children

The Services are not directed to, and we do not knowingly collect personal data from, individuals under the age of 18. If we become aware that we have collected personal data from someone under 18, we will take steps to delete that information.

11. Changes to This Policy

We may update this Policy from time to time. We will notify you of material changes in the manner described in our Terms and Conditions. The date at the top of this Policy indicates when it was last updated.

12. Contact Us and Complaints

If you have any questions about this Policy or wish to exercise any of your rights, please contact our Data Protection Officer at dpo@monavateonchain.com. If you are not satisfied with our response, you have the right to lodge a complaint with your national data protection supervisory authority, or with the Data Protection Commission of Ireland at www.dataprotection.ie, without prejudice to any other administrative or judicial remedy.