Privacy Policy

Last Updated: March 5, 2025

This Privacy Policy ("Policy") describes how Myfye ("**Myfye**," "**we**," "**us**," or "**our**") collects, uses, and discloses personal information, and explains your rights regarding this information. We are committed to protecting your privacy and complying with applicable data protection laws. If you have any questions about this Policy or our data practices, please contact us using the information in the **Contact Information** section below.

Applicability of This Policy

This Policy applies to personal information we collect through Myfye's mobile application, website, and related services (collectively, the "**Services**"). By using the Services, you agree to the terms of this Privacy Policy. **Do not use the Services if you do not agree with this Policy.** This Policy does not cover any third-party websites or services that integrate with Myfye except as described here. It also does not apply to any information collected from job applicants or employees in a work context. This Policy is not a contract and does not create any legal rights or obligations beyond those under applicable law.

Types of Data We Collect

We collect various types of personal data ("Personal Information") from you or about you, as described below. The specific information we collect depends on how you interact with our Services.

Information You Provide

We collect Personal Information that you provide directly to us when using Myfye, such as:

- **Identity and Contact Information:** Your full legal name, email address, phone number, date of birth, and physical address. This includes any contact details you provide when creating an account or contacting customer support.
- **KYC Information:** As part of our Know Your Customer (KYC) process (performed by our provider Persona), we may collect government-issued identification documents (e.g. passport or driver's license), a facial scan or selfie for identity verification, and proof of address (such as a utility bill or bank statement). **All KYC information is collected and processed on our behalf by Persona (our identity verification partner).**
- **Financial Information:** Details necessary for transactions on Myfye, such as cryptocurrency wallet addresses and transaction history. If you use our fiat on/off ramp Services (powered by BlindPay), we may collect payment details like bank account information or transaction references required to facilitate deposits or withdrawals.

- **User Communications:** The content of your communications with us, including support requests, feedback, or survey responses. If you contact us via email or in-app chat, we will collect the information you choose to provide in those interactions.

Information We Collect Automatically

Like many mobile applications, Myfye and our third-party providers automatically collect certain information about your device and usage of the Services:

- **Device and Technical Information:** This includes device identifiers (such as device ID or unique device token), device type, operating system and version, mobile network information, and application version. We also collect your Internet Protocol (IP) address and **geolocation** derived from your IP or device settings (at a coarse city or country level) to detect fraud and comply with regional requirements.

- **Usage Data:** We record information about your activity on the app, such as features you use, pages or screens viewed, links or buttons clicked, and the dates/times of your visits. For example, we may log when you initiate a token swap or view your wallet balance. This usage data helps us analyze and improve our Services.

- **Cookies and Similar Technologies:** If you use our website or web-based interfaces, we may use cookies or similar tracking technologies to remember your preferences and authenticate your session. **Myfye does not use third-party analytics or advertising trackers by default.** However, essential cookies or local storage may be used for things like keeping you logged in and ensuring the app functions properly. You can configure your browser or device to block or alert you about these technologies, but some parts of the Service may not work correctly without them.

Information from Third Parties

We may receive Personal Information about you from third-party sources in connection with providing our Services, including:

- **Identity Verification Services:** As noted, we use Persona for KYC. When you submit your identity documents and proof of identity through Persona's interface, Persona verifies this information and shares with us a confirmation of your identity and KYC status (e.g. pass/fail and related verification details). Persona may also provide fraud or sanctions screening results as part of compliance checks.

- **Transaction Partners:** If you engage in token swaps or fiat conversions, certain data about those transactions may come from our partners. For example, **Jupiter** (our token swap provider) may provide data on swap rates or route your transaction through various decentralized exchanges, and **BlindPay** (our fiat ramp provider) may give us status updates on your deposit or withdrawal (such as confirmation that funds were received or sent). These partners generally receive the information needed to execute the transaction (such as your wallet address, transaction amount, and asset type) and then provide us relevant confirmations or details.

- **Other Service Providers:** We may receive supplemental information from service providers that support our platform operations. For instance, if we use cloud hosting or security services, they might incidentally collect log data or error reports which we have access to. We treat any information obtained from such providers in accordance with this Policy.

We combine information from these third-party sources with the information we collect directly from you for the purposes described in this Policy.

Purpose of Collection (How We Use Your Information)

Myfye uses the collected information for various business and operational purposes consistent with applicable law. The primary purposes for which we collect and process Personal Information include:

- **Providing and Enhancing the Service:** We use your information to create and manage your Myfye account, enable the core functionality of our app (such as your crypto wallet and token swaps), and facilitate transactions you request. For example, your identity and contact info allow you to register and log in, and your financial information allows us to process crypto or fiat transactions. We also use data about how you use Myfye to improve and personalize your experience, fix bugs, and develop new features.

- **Identity Verification and Legal Compliance:** We process your Personal Information to verify your identity, fulfill KYC and anti-money laundering (AML) obligations, and ensure compliance with financial regulations. Government ID details, facial scans, and proof of address are used (via Persona) to confirm your identity and screen for fraud or unlawful activity. We may also use your information to satisfy other legal requirements – for instance, keeping records of transactions as required by law, or responding to lawful requests by authorities.

- **Transactions and Services Delivery:** Information like your wallet addresses, transaction history, and bank details (for fiat ramps) is used to execute the operations you request. This includes conducting token swaps through Jupiter's integration, and processing deposits/withdrawals via BlindPay. We share the necessary data with these processors to complete your transactions and ensure they are carried out correctly and securely.

- **Safety, Security, and Fraud Prevention:** We may use your data to protect the integrity of the platform, our users, and their assets. This includes using device info, IP addresses, and usage patterns to detect and prevent fraud, unauthorized access, security breaches, or other potentially illegal or prohibited activities. For example, we might flag suspicious login attempts or multiple failed transactions for review. We also enforce our Terms of Service and other policies by monitoring for violations using relevant data.

- **User Support and Communications:** We will use your contact information to communicate with you about your account and the Services. This includes sending critical **service-related communications** such as transaction confirmations, alerts about important changes or security issues, and responses to your support inquiries. We also use the

information you provide in communications (like emails or support chats) to address your questions, troubleshoot issues, and improve our support processes.

- **Marketing and Product Updates (with Opt-In Consent):** If you **opt in** to receive marketing or promotional communications, we will use your email or other provided contact to send you product updates, newsletters, offers, or event announcements related to Myfye. We will only send you such communications if you have given consent (for example, by toggling on marketing messages in your app settings or checking an opt-in box). You can withdraw your consent at any time (see **Opt-In for Communications** below). We do *not* use your data for third-party advertising targeting, and we do not share your data with advertisers.

- **Research and Development:** Aggregated and de-identified information (which cannot reasonably be linked back to you) may be used for internal analytics and product development. For instance, we might aggregate usage statistics to understand how users interact with a new feature, so we can make improvements. When we use data for these purposes, we remove or anonymize any personal identifiers.

- **Legal Reasons:** We may use or disclose your information as necessary to exercise or defend legal claims, comply with subpoenas, court orders, or other legal process, and to protect our rights, property, or safety as well as those of our users or others. This includes using data to investigate or prevent fraud and other unlawful activities, or as part of a business transaction (such as a merger, acquisition, or financing) where information might be reviewed under appropriate confidentiality safeguards.

We will only use your Personal Information for the purposes above and will obtain your consent before using it for any purpose that is incompatible with these, unless otherwise permitted or required by law.

Third-Party Processors and Data Sharing

Myfye **does not sell your personal data** to third parties. We only share your information in limited situations, such as with third-party service providers and processors who assist us in operating the Services, or as required by law. These third parties are bound by contractual obligations to process Personal Information only on our behalf and to protect it. The key third-party processors we use include:

- **Persona (Identity Verification):** We partner with Persona for performing KYC checks. When you submit KYC documents and information through our app, you are actually providing them to Persona via an embedded interface. Persona collects and processes your ID documents, biometric data (facial scan), and other KYC information on our behalf to verify your identity and perform compliance screening. Persona then shares the verification results with Myfye. Persona may retain copies of your KYC data as required for compliance. (See Persona's privacy policy for details on their data handling.) We only receive the data from Persona necessary to establish your verified status and comply with record-keeping laws.

- **Privy (Wallet Infrastructure):** We use Privy to power Myfye's embedded crypto wallets. Privy helps us create and manage cryptographic wallet keys securely for each user. In providing this service, Privy may handle certain user identifiers (such as your user ID, public wallet address, or encrypted keys) to ensure you can seamlessly access your wallet through the Myfye app. Privy does **not** receive your sensitive personal details like name or ID – those stay with Myfye/Persona. Privy's role is limited to managing technical wallet data under strict security controls.

- **Jupiter (Token Swap Service):** Jupiter is integrated into Myfye to enable cryptocurrency token swaps (trades between different tokens). When you initiate a swap, Myfye uses Jupiter's API to find the best exchange rates and execute the swap via supported decentralized exchanges. For this purpose, Myfye shares the necessary transaction data with Jupiter (such as the tokens you want to trade, amounts, and your public wallet address to receive the output). Jupiter processes that data to perform the swap and returns the result to Myfye. Jupiter does not collect identifying information like your name or contact details from us – only the data required to carry out the token exchange.

- **BlindPay (Fiat On/Off Ramps):** BlindPay is our partner for converting between fiat currency and cryptocurrency (e.g. swapping USD and stablecoins). If you choose to deposit fiat currency to buy crypto or withdraw crypto into fiat, the transaction is handled by BlindPay's payment infrastructure. This means Myfye shares information like your linked wallet address, the amount of money to be transferred, and relevant payment instructions with BlindPay. In some cases, BlindPay may require additional information to process a transfer, such as your bank account details for a wire transfer or confirmation that KYC is completed. BlindPay may also perform its own compliance checks (e.g. screening transactions for fraud or sanctions) as part of processing. We only share with BlindPay what is necessary for your requested transaction, and BlindPay is not permitted to use your data for any other purpose.

- **Cloud Storage and Other Vendors:** We host Myfye's data and backend on secure servers in the United States (for example, using reputable cloud service providers). These providers may technically process or store Personal Information as needed for data hosting and backup. Additionally, we might use other vendors for services like email delivery (to send verification codes or notices) or customer support software. Whenever we engage an additional service provider that needs access to Personal Information, we do so under a contract that protects your information and meets applicable privacy requirements.

Aside from the service providers above, we will only disclose your Personal Information to third parties in a few exceptional scenarios: **(a)** if you specifically request or consent to the disclosure (for example, if you use a feature that asks us to share data with a friend or another app, we will do so with your direction); **(b)** if we are required by law or legal process to disclose information (such as responding to a court order, regulatory inquiry, or lawful government request); or **(c)** in connection with a corporate transaction, such as a merger, acquisition, or sale of assets, where your information may be transferred to a successor entity under appropriate confidentiality and legal safeguards. In all such cases, we will ensure any third party has a legal obligation to keep your information secure and confidential.

Myfye does not share your personal data with third parties for their own marketing purposes, and we never sell your information to data brokers or advertisers.

International Data Transfers

Myfye is based in the United States, and the Personal Information we collect is stored and processed on servers located in the U.S. If you are using the Services from outside the United States, be aware that your information will be transferred to and maintained on servers or databases within the U.S. or other jurisdictions where our service providers are located. These jurisdictions may have data protection laws that are different from (and potentially less protective than) the laws in your country of residence.

However, regardless of where your data is processed, we will protect it as described in this Privacy Policy and in accordance with applicable law. When we transfer Personal Information from the European Economic Area (EEA), United Kingdom, or other regions with data transfer restrictions, we take steps to ensure appropriate safeguards are in place. This may include using standard contractual clauses approved by the European Commission, relying on the service provider's certification under relevant data protection frameworks, or obtaining your explicit consent where required by law. By using Myfye's Services or providing us with your information, you acknowledge the transfer of your personal data to the United States and other jurisdictions as necessary for our legitimate business purposes.

Your Rights and Choices

You have certain rights and choices regarding your Personal Information, especially if you are located in jurisdictions with robust privacy laws such as the European Union (under the General Data Protection Regulation **GDPR**) or California (under the California Consumer Privacy Act **CCPA**). We honor all individuals' rights as applicable under relevant data protection laws. These rights may include:

- **Access and Portability:** You have the right to request a copy of the Personal Information we hold about you, and to receive it in a commonly used electronic format. This helps you to review the information and, in some cases, transfer it to another service.

- **Correction:** You may ask us to correct or update any inaccurate or incomplete Personal Information we have about you. We encourage you to keep your account information up-to-date, and you can often make certain changes directly in the app.

- **Deletion:** You can request that we delete your Personal Information. Upon request, we will erase your data from our records, provided we do not have a legal obligation or compelling legitimate interest to retain it. For example, we may need to keep certain transaction records to comply with financial regulations or dispute resolutions, even if you close your account – but we will inform you if such an exception applies.

- **Restriction of Processing:** You have the right to ask us to restrict or pause the processing of your Personal Information in certain circumstances – for instance, if you contest the

accuracy of the data or object to our processing. We will limit processing to storage and necessary activities only, as required by law.

- **Objection to Processing:** In some jurisdictions, you may have the right to object to our processing of your Personal Information, particularly if we are processing it based on a legitimate interest (or performing direct marketing). If you raise an objection, we will evaluate it and refrain from further processing your information for that purpose unless we have a compelling legitimate ground or a legal necessity to continue.

- **Withdraw Consent:** If we rely on your consent to process any Personal Information (such as for optional marketing communications), you have the right to withdraw that consent at any time. Withdrawing consent will not affect the lawfulness of any processing we already conducted based on your prior consent.

- **Non-Discrimination:** If you exercise any of the above rights, we will not discriminate against you or deny you our Services as a result. For example, if you opt out of marketing emails, we will not downgrade your account or reduce your access to features.

To exercise your rights, please contact us at the email address provided in **Contact Information** below. We may need to verify your identity before fulfilling certain requests (to ensure we do not disclose your data to someone else). We will respond to your request within the timeframe required by applicable law (for example, within 30 days for GDPR requests, or 45 days for CCPA requests, with the possibility of a reasonable extension). If we cannot fulfill your request in whole or in part, we will provide an explanation. For instance, we might decline a deletion request if retaining certain data is necessary to comply with a legal obligation.

In addition to the above, users in some jurisdictions have the right to lodge a complaint with a data protection authority if they believe our processing of their Personal Information violates the law. We encourage you to contact us first so we can address your concerns directly.

Data Retention

We retain Personal Information for as long as necessary to fulfill the purposes for which it was collected, unless a longer retention period is required or permitted by law. In general, this means we will keep your information for the duration of your account being active and for a reasonable period thereafter. For example, if you close your Myfye account, we may still retain certain data for a period of time to finalize any pending transactions, to comply with record-keeping regulations (such as financial and anti-money laundering laws that mandate keeping transaction or KYC data for a minimum number of years), to resolve disputes, or to enforce our agreements.

When Personal Information is no longer needed for the purpose it was collected, and we are not legally required to retain it, we will either delete, anonymize, or securely isolate that data. If deletion is not immediately feasible (for example, because the data is stored in backup archives), we will safeguard the data and restrict any active use of it until it can be deleted.

Data Security

Myfye takes the security of your Personal Information seriously. We implement administrative, technical, and physical safeguards designed to protect your data from unauthorized access, theft, loss, misuse, or alteration. These measures include, for example: encrypting sensitive data both in transit (using TLS/SSL) and at rest, restricting access to Personal Information to authorized personnel who have a legitimate need to know, using authentication procedures and access controls in our app and servers, and continuously monitoring our systems for potential vulnerabilities or attacks.

We also rely on trusted third-party infrastructure with strong security practices (such as our cloud hosting providers and security services). Our third-party processors (Persona, Privy, Jupiter, BlindPay, etc.) are vetted to ensure they meet industry security standards to protect the data we entrust to them.

Despite our efforts, no security measure or method of data transmission can be guaranteed to be 100% secure. The internet and blockchain networks by their nature carry inherent risks. **You are responsible for maintaining the security of your account credentials and wallet keys** on Myfye. We encourage you to use unique, strong passwords and enable any available security features (like two-factor authentication) to help protect your account. If you suspect any unauthorized access to or use of your account, please notify us immediately.

In the event of a data breach or security incident affecting your Personal Information, we will act promptly to mitigate the impact and notify you and relevant authorities as required by law.

Opt-In for Communications

Myfye strives to respect your preferences regarding communications. By default, we will send you only **transactional or service-related communications** – for example, confirming a money transfer, alerting you to important changes in the Services, sending password resets, or informing you of updates to this Privacy Policy or our Terms of Service. These are necessary communications for using the Myfye platform and are not optional as long as you maintain an account.

For **marketing communications** (such as product updates, newsletters, new feature announcements, or promotions), we operate on an **opt-in** basis. This means we will **only** send you marketing emails, SMS, or push notifications if you have expressly agreed to receive them. You may have given this consent when signing up (e.g., by checking a box to receive news and offers) or by adjusting your user settings to enable marketing messages.

If you have opted in to marketing communications, you have the right to opt out at any time. You can unsubscribe from our emails by clicking the “unsubscribe” link typically provided at the bottom of each marketing email. For SMS or push notifications, you can follow the instructions in the message to stop further messages (for example, replying “STOP” to an SMS), or disable these notifications in your app settings. You can also contact us directly to request removal from our marketing list.

Please note that opting out of marketing or promotional communications will **not** affect your receipt of important service-related communications from Myfye. We may still send you non-

promotional messages as needed for customer service, security, or legal notification purposes (as described above in **User Support and Communications**).

Myfye does not engage in unsolicited marketing and does not share your contact information with third parties for them to market to you. All promotional communications you receive from Myfye will come directly from us in accordance with your preferences. If you believe you are receiving communications you did not sign up for, please let us know so we can investigate and resolve the issue.

Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements, or for other operational reasons. If we make changes, we will update the "Last Updated" date at the top of the Policy. **We encourage you to review this Policy periodically** to stay informed about how we are protecting your information.

For any significant or material changes that affect your rights or the way we handle your Personal Information, we will provide a more prominent notice. This could include posting a notice within the Myfye app, sending an email to the address associated with your account, or other appropriate communication methods. If required by law, we will also obtain your consent to any material Privacy Policy changes.

Your continued use of the Services after the revised Policy has become effective indicates that you have read and understood the current version of this Privacy Policy.

Contact Information

If you have any questions, concerns, or requests regarding this Privacy Policy or Myfye's handling of your Personal Information, please **contact us**. We are here to help and will respond within a reasonable timeframe, in accordance with applicable laws.

- **Email:** You can reach our privacy team at eli@myfye.com. This is the primary channel for privacy-related inquiries or to exercise your data subject rights (access, deletion, etc.).
- **In-App Support:** You may also contact us through the Myfye app's support chat or contact form. Simply mention that your request is related to privacy or personal data, and it will be routed to the appropriate team.

We will gladly answer your questions and work to resolve any issues you have regarding your privacy. If you need to exercise any rights over your data, please make clear what information or action you are requesting, and we will guide you through any verification or process steps. Thank you for trusting Myfye with your personal information; we are committed to keeping that trust.