

# PRIVACY POLICY

*Last updated: 7 May 2026*

Arvo ("Arvo", "we", "us" or "our") is committed to providing the highest level of privacy and security regarding collection and use of our customers' personal information. This policy describes how we may collect, use and disclose your personal information.

This Privacy Policy applies to:

- this website and any pages, portals, dashboards, forms, or microsites we operate that link to it, as applicable;
- our mobile or web applications that link to it; and
- the businesses and brands listed below that are presented on or accessible via this website:
  - **Arvo Limited** (License number CL12394) whose registered address is at GD-PB-04-01-OF-01-0, Level 1, DIFC Fund Centre, Gate District Precinct Building 04, Dubai International Financial Centre, Dubai, UAE.

## Introduction

Arvo is a property crowdfunding platform that enables retail and accredited investors to invest in Dubai real estate from as little as USD 100. We are licensed and regulated by the Dubai Financial Services Authority (DFSA) and operate from the Dubai International Financial Centre (DIFC).

As a regulated financial services provider, we collect and process personal data in order to deliver our services, comply with our legal and regulatory obligations (including know-your-customer (KYC), anti-money laundering (AML) and counter-terrorist financing (CTF) requirements), and protect our customers, our platform and our community from fraud and financial crime.

We process personal data in accordance with the DIFC Data Protection Law No. 5 of 2020 (the "DIFC DP Law") and, where applicable, the EU General Data Protection Regulation (GDPR), the UK GDPR, and other applicable data protection laws.

## Purpose of a Privacy Policy

The purpose of this Privacy Policy is to explain, in a clear and transparent way:

- what personal data we collect about you;
- how and why we collect, use, share and store that data;
- the legal bases on which we rely to process your personal data;
- how long we keep your personal data;
- the rights you have in relation to your personal data; and
- how you can contact us if you have any questions or concerns.

You should read this Privacy Policy together with any other policies or notices we provide to you at the time we collect or process your personal data, including our Terms and Conditions and Cookies Policy.

## How do we collect and use your personal data?

### Categories of personal data we collect

Depending on how you interact with us, we may collect the following categories of personal data:

- **Identity data:** full name via KYC provider. Date of birth, place of birth, nationality, gender, photograph, passport and in some cases other government-issued identification (residence visa or driver's licence) remains with the KYC provider.
- **Contact data:** email address. Residential address is confirmed and remains with the KYC provider.
- **Financial and investment data:** source of funds, source of wealth, employment and income information, bank account details, transaction history, investment activity on the platform, holdings, distributions and tax-related information.
- **Verification and due diligence data:** information collected through KYC, AML, CTF, sanctions and adverse media screening, including biometric facial verification data captured during onboarding.
- **Account data:** email, account preferences, communication preferences and authentication logs.
- **Technical and device data:** IP address, device identifiers, browser type and version, operating system, time zone, language, referring URLs, pages visited, session duration and clickstream data.
- **Communications data:** correspondence with our customer support team, recordings of calls (where notified), in-app messages and feedback you provide.
- **Marketing data:** your preferences in receiving marketing from us, your communication preferences and your engagement with our marketing communications.

### How we collect your personal data

We collect personal data:

- **directly from you** when you register an account, complete onboarding, make an investment, contact us, or otherwise interact with our website or app;
- **automatically** through cookies, server logs and similar technologies when you use our website or app;
- **from third parties** such as our identity verification provider (Sumsb), payment service providers (Tap Payments and Emirates NBD), sanctions and PEP screening

providers, public registers, government and regulatory authorities, and our service providers and partners.

## Purposes and legal bases for processing

We process your personal data for the following purposes and on the following legal bases:

- **To onboard you and provide our services:** this includes creating and maintaining your account, processing your investments, holding your funds via our banking partners, distributing returns and providing customer support. Legal basis: performance of a contract with you.
- **To comply with legal and regulatory obligations:** this includes KYC, AML, CTF, sanctions screening, suitability and appropriateness assessments, tax reporting, regulatory reporting to the DFSA and responding to lawful requests from authorities. Legal basis: compliance with a legal obligation.
- **To detect and prevent fraud and financial crime:** this includes transaction monitoring, fraud detection, risk scoring and security investigations. Legal basis: legitimate interests (protecting our platform, our customers and the integrity of the financial system) and compliance with a legal obligation.
- **To operate, secure and improve our platform:** this includes monitoring uptime, diagnosing issues, improving user experience and developing new features. Legal basis: legitimate interests (running and improving our business).
- **To communicate with you:** this includes sending service announcements, regulatory notices, statements and responses to your queries. Legal basis: performance of a contract and legitimate interests.
- **For marketing:** this includes sending you newsletters, product updates and information about new investment opportunities. Legal basis: your consent and/or our legitimate interests, depending on the channel and applicable law.
- **To establish, exercise or defend legal claims** and to enforce our terms. Legal basis: legitimate interests and, where relevant, compliance with a legal obligation.

## Personal and Sensitive User Data

Some of the data we collect is considered "special categories of personal data" or "sensitive personal data" under the DIFC DP Law and the GDPR. This may include biometric data captured during identity verification (for example, facial scans collected by our verification provider, Sumsu).

We process such data only where we have a lawful basis to do so, which will typically be:

- your explicit consent (where required); or
- the establishment, exercise or defence of legal claims; or
- reasons of substantial public interest, including the prevention of financial crime.

We apply additional safeguards to sensitive personal data, including stricter access controls and shorter retention where permitted.

## How do we safeguard your personal data?

We take the security of your personal data seriously and have implemented appropriate technical and organisational measures designed to protect it against unauthorised or unlawful processing, accidental loss, destruction, damage, alteration or disclosure. These measures include:

- encryption of personal data in transit (TLS) and at rest;
- strict role-based access controls and the principle of least privilege;
- multi-factor authentication for access to our systems;
- regular vulnerability scanning, penetration testing and security reviews;
- secure software development practices and code review;
- staff training on data protection, information security and confidentiality;
- vendor due diligence and contractual data protection commitments with our processors; and
- incident response and breach notification procedures.

Despite our efforts, no method of transmission over the internet or method of electronic storage is completely secure. If you have reason to believe that your interaction with us is no longer secure, please contact us immediately at [compliance@arvo.co](mailto:compliance@arvo.co).

## How long do we retain your personal data for?

We keep your personal data only for as long as necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, regulatory, accounting or reporting requirements. As a DFSA-regulated firm, we are subject to minimum record-keeping obligations.

Our standard retention periods are as follows:

- **KYC, AML, CTF and onboarding records:** 6 years from the end of our business relationship with you, or longer where required by applicable law or by the DFSA.
- **Transaction and investment records:** 6 years from the date of the transaction.
- **Account data:** 6 years from closure of your account.
- **Marketing data:** until you withdraw your consent or object to direct marketing, after which we will retain a minimal suppression record so that we do not contact you again.
- **Website analytics data:** typically up to 26 months from collection.
- **Customer support communications:** typically up to 3 years from the date of the last interaction, unless a longer period is required to handle a complaint, dispute or legal claim.

When we no longer need your personal data, we will securely delete it or anonymise it so that it can no longer be associated with you.

## Who do we disclose your personal data to?

We do not sell your personal data. We may share your personal data with the following categories of recipients, in each case under appropriate contractual and security safeguards:

### Service providers and processors

We use carefully selected third-party service providers to help us deliver our services. Our key processors include:

- **Identity verification:** Sumsub (KYC, AML, biometric verification and sanctions screening).
- **Payments and banking:** Tap Payments (payment processing) and Emirates NBD (banking and account services).
- **Email and communications:** Mailchimp (marketing email), Postmark (transactional email) and Google Workspace (corporate email and productivity).
- **Cloud hosting and infrastructure:** our cloud and infrastructure providers, who host the platform and supporting systems.
- **Analytics and product tooling:** analytics providers that help us understand how our platform is used and improve it.

### Group companies and partners

We may share your personal data with affiliates within the Arvo group of companies and with property partners, special purpose vehicles (SPVs), fund administrators, trustees and custodians where this is necessary to administer your investments.

### Regulators and authorities

We may share your personal data with the Dubai Financial Services Authority (DFSA), the DIFC Authority, tax authorities, law enforcement, courts and other governmental or regulatory bodies where required by applicable law or where we believe in good faith that disclosure is necessary to comply with a legal obligation, protect our rights or the rights of others, or prevent fraud or other unlawful activity.

### Professional advisers and corporate transactions

We may share your personal data with our professional advisers (such as auditors, lawyers and accountants) and with potential or actual buyers, investors, lenders or successors in the context of a corporate transaction (such as a merger, acquisition, financing or sale of assets), in each case under appropriate confidentiality obligations.

## How do you withdraw your consent including marketing opt-out?

Where we rely on your consent to process your personal data (for example, for direct marketing communications by email), you can withdraw your consent at any time.

Withdrawing your consent will not affect the lawfulness of any processing we carried out before you withdrew your consent.

You can opt out of marketing communications by:

- clicking the "unsubscribe" link in any marketing email we send you;
- updating your communication preferences in your account settings; or
- contacting us at [compliance@arvo.co](mailto:compliance@arvo.co).

Please note that even if you opt out of marketing communications, we will still send you service-related communications (such as transaction confirmations, statements, regulatory notices and security alerts) where these are necessary for us to provide our services or comply with our legal obligations.

## **Do we carry out profiling and automated decision making?**

We use automated tools to support our fraud detection and financial crime risk management. This may include automated risk scoring of accounts and transactions, sanctions and PEP screening, and pattern-based fraud detection.

These automated tools support, but do not replace, human review. We do not make decisions that produce legal effects concerning you or similarly significantly affect you based solely on automated processing without human involvement. Where an automated alert is generated, a member of our compliance team reviews the alert and makes the final decision.

Where applicable law gives you a right to a human review of an automated decision, to express your point of view and to contest the decision, you may exercise that right by contacting us at [compliance@arvo.co](mailto:compliance@arvo.co).

## **Monitoring**

We monitor activity on our website, app and platform for security, fraud prevention, regulatory compliance and quality assurance purposes. This may include:

- logging access to and use of our platform;
- monitoring transactions for signs of fraud, money laundering or other financial crime;
- recording or monitoring telephone calls and electronic communications with our staff (where notified to you) for training, quality and compliance purposes; and
- monitoring our systems for security threats and unauthorised access.

We carry out monitoring in accordance with applicable law and only to the extent necessary and proportionate to the purposes described above.

## **What rights do you have?**

Subject to applicable law and to certain conditions and exemptions, you have the following rights in relation to your personal data:

- **Right of access:** to obtain confirmation of whether we process your personal data and a copy of that data.
- **Right to rectification:** to have inaccurate or incomplete personal data corrected.
- **Right to erasure ("right to be forgotten"):** to have your personal data deleted in certain circumstances.
- **Right to restrict processing:** to ask us to limit how we use your personal data in certain circumstances.
- **Right to data portability:** to receive your personal data in a structured, commonly used and machine-readable format and, where technically feasible, to have it transmitted to another controller.
- **Right to object:** to object to processing carried out on the basis of legitimate interests, and to object at any time to processing for direct marketing purposes.
- **Right to withdraw consent:** where we rely on your consent, to withdraw it at any time.
- **Right not to be subject to solely automated decisions:** that produce legal or similarly significant effects, except in limited circumstances.
- **Right to lodge a complaint:** with the DIFC Commissioner of Data Protection (<https://www.dp.difc.ae>) or, if you are in the EU/EEA or UK, with your local data protection supervisory authority.

Please note that some of these rights may be limited where, for example, we are required by law or by the DFSA to retain your data, or where the data is needed to establish, exercise or defend legal claims.

To exercise any of your rights, please contact us at [compliance@arvo.co](mailto:compliance@arvo.co). We may need to verify your identity before responding to your request. We will respond within the timeframes required by applicable law.

## Third party websites

Our website and app may contain links to third-party websites, plug-ins and applications (for example, links to property partners, payment providers or social media platforms). Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements or practices. We encourage you to read the privacy policy of every website you visit.

## Social media

We maintain a presence on a number of social media platforms (such as LinkedIn, Instagram, X (formerly Twitter) and similar). When you interact with us on these platforms, the relevant platform may collect personal data about you in accordance with its own privacy policy, and may share certain information with us (for example, your profile information, comments and engagement metrics).

Where we and the social media platform are joint controllers, we will make available the essential terms of our arrangement on request. Otherwise, the social media platform is the controller for the personal data it collects through its platform and you should review its privacy policy.

## **International data transfers**

Some of our service providers and group companies are located outside the DIFC and the United Arab Emirates. As a result, your personal data may be transferred to, and processed in, jurisdictions other than the one in which you are located. These jurisdictions may have data protection laws that differ from those of the DIFC.

Where we transfer your personal data outside the DIFC, we will ensure that an adequate level of protection is in place by relying on one or more of the following safeguards:

- transfer to a jurisdiction recognised by the DIFC Commissioner of Data Protection as providing an adequate level of protection;
- the use of approved standard contractual clauses or equivalent contractual safeguards;
- binding corporate rules; or
- any other lawful transfer mechanism permitted under the DIFC DP Law and applicable data protection laws.

You may request further information about the safeguards we have put in place by contacting us at [compliance@arvo.co](mailto:compliance@arvo.co).

## **Changes to this privacy policy**

We may update this Privacy Policy from time to time to reflect changes in our practices, services, technology, legal requirements or other factors. When we make changes, we will update the "Last updated" date at the top of this policy. Where the changes are material, we will provide you with a more prominent notice (for example, by email or through a notice on our website or app) before the changes take effect.

We encourage you to review this Privacy Policy periodically to stay informed about how we are protecting your personal data.

## **Contact**

If you have any questions, comments or requests regarding this Privacy Policy or how we handle your personal data, or if you wish to exercise any of your rights, please contact our Data Protection Officer:

### **Arvo Limited**

Attn: Data Protection Officer

GD-PB-04-01-OF-01-0, Level 1

DIFC Fund Centre, Gate District Precinct Building 04

Dubai International Financial Centre

Dubai, United Arab Emirates

**Email:** [compliance@arvo.co](mailto:compliance@arvo.co)

You also have the right to lodge a complaint with the DIFC Commissioner of Data Protection at <https://www.dp.difc.ae> if you believe that our processing of your personal data does not comply with applicable data protection law.