Baanx.com LTD Privacy Policy

baanxuk.com
Last updated: June 2026
Effective date: June 2026 | Version 2026.1

The protection of the personal data of our customers and visitors to our websites and apps is important to Baanx. This Privacy Policy describes how we collect, use, share and protect your personal data when you access our services, including content on the baanxuk.com website and any other websites, pages, features or content owned or operated by us (collectively, the "Website"), or when you use our mobile applications, any associated cards, any API or third-party applications based on such API, and related services (together, the "Services").

Please read this Privacy Policy carefully. It should be read together with our Terms and Conditions, our Cookie Policy and any product-specific terms or notices we provide to you. If you have any questions about this Privacy Policy, you can contact us using the details in the "How to Contact Us" section below.

Use of the words "Baanx," "we," "us" or "our" refers to Baanx.com Ltd and, where relevant, its group companies and affiliates. We may change this Privacy Policy from time to time; you can always find the latest version on this page.

1. Who We Are and Our Regulatory Status

Baanx.com Ltd is the data controller responsible for your personal data in connection with the Services described in this Privacy Policy. We are a company registered in England and Wales with our registered office at The Officers Mess Business Centre, Royston Road, Duxford, Cambridge, England, CB22 4QH.

Baanx.com Ltd is registered with the Financial Conduct Authority (the "FCA") as a cryptoasset business under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, with Firm Reference Number (FRN) **927401**. You can verify our registration on the FCA Financial Services Register at register.fca.org.uk. Our registration relates to compliance with anti-money laundering and counter-terrorist financing obligations; cryptoassets are largely unregulated in the UK and the FCA does not approve the cryptoasset products or services we offer.

Some fiat (e-money and payment) services made available through the Services may be provided by a regulated partner acting as a separate controller or as a payment/e-money institution. Where that is the case, we will tell you and the relevant partner's own privacy notice may also apply. The table below sets out which entity controls your personal data depending on the services you use and where you live:

Your place of residence	Services provided	Controlling entity
United Kingdom	Cryptoasset / digital asset services	Baanx.com Ltd, The Officers Mess Business Centre, Royston Road, Duxford, Cambridge, England, CB22 4QH. Registered with the FCA as a cryptoasset business (FRN 927401).
United Kingdom	Fiat (e-money / payment) services	Monavate Ltd, The Officers Mess Business Centre, Royston Road, Duxford,

Your place of residence	Services provided	Controlling entity
		Cambridge, England, CB22 4QH (where fiat services are provided by our regulated partner).

2. The Personal Data We Collect

"Personal data" means any information that identifies, or is reasonably capable of identifying, an individual, directly or indirectly. We collect personal data in the following ways.

2.1 Personal data you provide to us

- **Identification information** — such as name, email address, telephone number, postal address, date of birth, nationality and government-issued identification numbers (for example passport, driving licence or national insurance number).
- **Financial information** — such as bank account details, sort code and account number, card details, bank statements and utility bills.
- **Commercial and transaction information** — such as trading activity, order activity, deposits, withdrawals and account balances.
- **Correspondence** — information you provide when you contact us, including during account opening and customer support.
- **Sensory information** — such as images and video collected for identity verification and audio recordings of calls.
- **Employment and source-of-wealth information** — such as job title and source of wealth or funds.
- **Institutional information** — for business customers, additional information such as the institution's legal name, company registration number, and proof of legal existence (for example articles of incorporation, certificate of incorporation, business licence or trust instrument).

2.2 Personal data we collect automatically

- **Online identifiers** — such as IP address and domain name.
- **Device information** — such as hardware, operating system and browser.
- **Usage data** — such as system activity, the pages and features you use and clickstream information.
- **Geolocation data** — approximate location derived from your device or IP address.

Our automatic collection of personal data may involve the use of cookies and similar technologies, described in section 8 below.

2.3 Personal data we collect from third parties

We may collect and/or verify personal data about you from third parties, including identity verification and fraud-prevention providers, sanctions-screening agencies, payment service providers, our partners and publicly available sources. We do not carry out credit or creditworthiness checks on you. The categories of personal data we obtain from third parties include:

- **Identification and financial information** — to verify your identity and the information you provide.
- **Transaction information** — including public blockchain data. Please note that cryptoasset transactions are not truly anonymous: parties who can match your public wallet address to other personal data may be able to identify you from a blockchain transaction, and analysis techniques applied to a blockchain may reveal further information about you.
- **Additional information** — at the discretion of our Compliance Team to meet our legal obligations, which may include information about criminal convictions, offences or alleged criminal activity, sanctions and politically exposed person (PEP) status.

Personal data you provide during the registration process may be retained even if your registration is left incomplete or abandoned.

2.4 Accuracy and retention

We take reasonable and practicable steps to ensure that the personal data we hold is accurate having regard to the purposes for which it is used, and is not kept for longer than is necessary for those purposes. See section 7 for more detail on retention.

2.5 Whether you have to provide your personal data

Some of the personal data we ask for is required by law — for example, the identity and verification information we must collect to meet our anti-money laundering obligations — and some is necessary for us to enter into and perform our contract with you. When you register for the Services, you are required to provide and verify a valid email address and mobile telephone number, as these are necessary to open, secure and operate your account and to contact you about it (see section 9). If you do not provide the personal data we request, we may be unable to open your account, provide some or all of the Services, or meet our legal and regulatory obligations.

3. Our Lawful Bases for Processing

We only process your personal data where we have a lawful basis to do so under the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018. The lawful bases we rely on are:

- **Legal obligation** — to carry out anti-money laundering, counter-terrorist financing, identity verification, sanctions screening, fraud prevention and reporting, and to meet our retention and regulatory obligations (Article 6(1)(c)).
- **Performance of a contract** — to satisfy our obligations to you under our Terms and Conditions, including opening and operating your account and providing customer support (Article 6(1)(b)).
- **Legitimate interests** — to monitor and secure our Services, carry out automated and manual security checks, prevent fraud, improve and develop our products, and protect our rights and those of our customers (Article 6(1)(f)). Where we rely on legitimate interests, we balance those interests against your rights and freedoms.
- **Consent** — for certain direct marketing and where otherwise required. You may withdraw your consent at any time without affecting the lawfulness of processing carried out before withdrawal (Article 6(1)(a)).

Where we process special category data (for example biometric data used for identity verification) or information relating to criminal convictions and offences, we do so only where an additional condition under the UK GDPR and the Data Protection Act 2018 applies, such as the prevention and detection of unlawful acts, compliance with regulatory requirements, or your explicit consent.

4. How We Use Your Personal Data

We use your personal data to provide a secure, compliant service, protect you and us from fraud, and improve our Services. In particular, we may use your personal data to:

- **Provide our Services** — to deliver the Services under our Terms and Conditions; for example, to facilitate transfers into and out of your account we need your financial information.
- **Comply with legal and regulatory requirements** — including identity verification and ongoing monitoring to meet our obligations under applicable anti-money laundering laws and FCA requirements.
- **Detect and prevent fraud and financial crime** — which is especially important given the irreversible nature of cryptoasset transactions.
- **Protect the security and integrity of our Services** — including monitoring your device and activity to keep your account secure.
- **Provide customer support** — whenever you contact our support team.
- **Optimise and improve our Services** — to understand how our products are used and to develop new products and features.
- **Communicate with you** — including service messages, and marketing where permitted (see section 9).
- **Other business purposes** — where the purpose is disclosed to you before collection or where you have given your consent.

5. How We Share Your Personal Data

We do not sell your personal data. We will only share your personal data as described below:

- **Service providers** — third parties who provide services to us such as identity verification, fraud detection and prevention, security threat detection, payment processing, customer support, data analytics, information technology, marketing, network infrastructure, storage, transaction monitoring and tax reporting, including providers who support our financial-regulation compliance. Our service providers are bound by strict confidentiality obligations and may only use your personal data to provide services to us.
- **Group companies and affiliates** — for the purposes described in this Privacy Policy and as necessary to provide the Services.
- **Co-brand and programme partners** — where you hold or access an account or product that is provided in partnership with, or under the brand of, one of our co-brand or programme partners, we share the personal data necessary to set up, service and administer that account with the relevant partner. This typically includes your name, email address and cryptoasset wallet address, and may include other information needed to operate the account, provide customer support and investigate and resolve disputes. We share this personal data on the basis of the performance of our contract with you and our (and our partner's) legitimate interests in operating the co-branded product. Each co-brand partner acts as an independent controller of the personal data we share with it, and the sharing is governed by a written data sharing agreement that sets out each party's

responsibilities. The partner's own privacy notice will also apply to its processing of your personal data.

- **Regulators, law enforcement and authorities** — where we are required or permitted to share your personal data with the FCA, HMRC, law enforcement, government officials and other regulators.
- **Corporate transactions** — in connection with a proposed or completed merger, acquisition, reorganisation, asset sale or similar transaction, or in the event of insolvency.
- **Professional advisers** — such as legal, accounting, audit and other consulting services to comply with our legal obligations.
- **With your consent** — where you have asked us or agreed to share your personal data.

6. International Data Transfers

We operate internationally and some of our systems, group companies and service providers are located outside the United Kingdom. Where we transfer your personal data outside the UK, we ensure an appropriate level of protection by relying on one of the following safeguards:

- **Adequacy** — transfers to countries that the UK government has determined provide an adequate level of data protection.
- **UK International Data Transfer Agreement (IDTA) or the UK Addendum** — to the European Commission's Standard Contractual Clauses, where adequacy does not apply.
- **Other lawful safeguards or derogations** — such as your explicit consent or where the transfer is necessary for the performance of our contract with you.

You can ask us for a copy of the safeguards we use for transfers of your personal data by contacting us using the details in section 15.

7. How Long We Keep Your Personal Data

We keep your personal data only for as long as is necessary for the purposes for which it was collected, including to meet our legal, regulatory, accounting and reporting requirements. As a firm subject to UK anti-money laundering law, we are generally required to retain customer due diligence records and transaction records for at least five years after the end of our business relationship with you, and in some cases longer where required by law or to establish, exercise or defend legal claims.

When personal data is no longer required, we will securely delete or anonymise it. For more detail, please see our Data Retention Policy.

8. Cookies and Similar Technologies

When you access the Website, we may place small data files known as cookies, together with pixel tags and similar tracking technologies, on your device. We use these to recognise you, remember your preferences, keep your account secure by detecting irregular or potentially fraudulent activity, support our anti-money laundering obligations, and assess and improve our Services and communications.

We set non-essential cookies only where you have given your consent, and you can manage your preferences through our cookie banner or your browser settings. You can learn more about cookies, including how to block them, at allaboutcookies.org. Please note that if you reject certain cookies, some features of the Website may not function properly.

9. Communications, Direct Marketing and Financial Promotions

Service and account communications. When you register for the Services you provide and verify your email address and mobile telephone number. We use these to send you service and account communications by email and SMS — for example, one-time passcodes and login or identity verification, security alerts, transaction confirmations, servicing messages, and important notices about your account or changes to this Privacy Policy or our terms. These communications are necessary to operate your account and to meet our security and legal obligations; they are not marketing, and you cannot opt out of them while you hold an account with us.

Direct marketing. Subject to applicable law, we may from time to time send you marketing communications about our products, services and features that we believe may be of interest to you, using the contact details you have provided. Where required by law we will only do so with your consent (or, for existing customers, in reliance on the limited “soft opt-in” permitted under the Privacy and Electronic Communications Regulations), and you can opt out of marketing at any time, without affecting our service and account communications, by using the unsubscribe link in our communications or by contacting us.

Any financial promotions we communicate or approve are subject to FCA rules, including the requirement that they are fair, clear and not misleading. We do not provide your personal data to third parties for their own direct marketing purposes without your consent.

10. Information Security

No security is foolproof and the internet is not a completely secure medium, so we cannot guarantee absolute security. However, we work hard to protect you and us from unauthorised access to, or unauthorised alteration, disclosure or destruction of, the personal data we hold. The measures we take include encryption of website communications using SSL/TLS, multi-factor authentication, periodic reviews of our data collection, storage and processing practices, and restricting access to your personal data on a need-to-know basis to employees, contractors and agents who are subject to strict confidentiality obligations.

If we become aware of a personal data breach that is likely to result in a risk to your rights and freedoms, we will notify the Information Commissioner’s Office and, where required, affected individuals, in line with our legal obligations.

11. Your Rights Under UK Data Protection Law

Under the UK GDPR and the Data Protection Act 2018, you have a number of rights in relation to your personal data. These rights are not absolute and may be subject to exceptions, in particular where we must retain or process data to meet our legal and regulatory obligations.

Your right	What it means
Right to be informed	To be told how we collect and use your personal data — which is the purpose of this Privacy Policy.
Right of access	To request a copy of the personal data we hold about you and certain information about how we process it.
Right to rectification	To have inaccurate personal data corrected and incomplete data completed.

Your right	What it means
Right to erasure	To ask us to delete your personal data in certain circumstances. This right is limited where we must keep data to meet legal, regulatory or anti-money laundering obligations.
Right to restrict processing	To ask us to limit how we use your personal data in certain circumstances.
Right to data portability	To receive certain personal data you provided to us in a structured, commonly used, machine-readable format, and to have it transmitted to another controller.
Right to object	To object to processing based on our legitimate interests, and to object to direct marketing at any time.
Rights relating to automated decision-making	Not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects, except as permitted by law and with appropriate safeguards.
Right to withdraw consent	Where we rely on consent, to withdraw it at any time. This does not affect the lawfulness of processing carried out before withdrawal.

To exercise any of these rights, please contact us using the details in section 15. We are legally required to verify your identity before responding, and may ask you for additional information to do so. We will respond within one month, although we may extend this by a further two months for complex or numerous requests, and we will let you know if we do. We do not usually charge a fee, but we may charge a reasonable fee or refuse to act on requests that are manifestly unfounded, excessive or repetitive.

If you are unhappy with how we have handled your personal data, you have the right to complain to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection, at ico.org.uk or by calling 0303 123 1113. We would, however, appreciate the chance to address your concerns before you approach the ICO, so please consider contacting us first.

12. Automated Decision-Making and Profiling

We may use automated processing, including profiling, as part of our identity verification, transaction monitoring and fraud-prevention controls. Where a decision that produces a legal or similarly significant effect on you is based solely on automated processing, we will only do so where it is permitted by law — for example, where it is necessary to enter into or perform our contract with you, or to comply with our legal obligations — and we will apply appropriate safeguards, including your right to obtain human intervention, to express your point of view and to contest the decision.

13. Children's Privacy

Our Services are not directed at children and are intended for individuals aged 18 or over. We do not knowingly collect personal data from anyone under 18. If you believe a child has provided us with personal data, please contact us and we will take steps to delete it.

14. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements or for other operational reasons. When we make material changes, we will update the "Last updated" date above and, where appropriate, notify you. We encourage you to review this page periodically. The latest version will always be available on this page.

15. How to Contact Us

If you have any questions or concerns about this Privacy Policy or how we handle your personal data, or if you wish to exercise your rights, please contact the relevant team below:

Data protection & compliance enquiries: compliance@baanxuk.com

Complaints: complaints@baanxuk.com

Fraud: fraud@baanxuk.com

Security: security@baanxuk.com

Customer support: support@baanxuk.com

General enquiries: contact@baanxuk.com

By post: Data Protection / Compliance, Baanx.com Ltd, The Officers Mess Business Centre, Royston Road, Duxford, Cambridge, England, CB22 4QH.

Complaints. If you wish to make a complaint about our Services, please contact complaints@baanxuk.com and we will handle it in accordance with our complaints procedure. Please note that, because the cryptoasset activities we carry on are not regulated financial services activities, complaints about them are not generally eligible for referral to the Financial Ombudsman Service.

If you believe we have not adequately resolved a data protection concern, you may contact the Information Commissioner's Office as described in section 11.