ABXWALLET.COM

PRIVACY POLICY

Version 4 — Last updated: 9 November 2026

This privacy policy explains how **HAYAT GORDEEV HOLDINGS EUROPE LTD** ("**ABX**", "**we**", "**us**" or "**our**") collects and uses personal data when you visit www.abxwallet.com or use ABX Wallet (the "**Service**"). It applies whether you run an account, are a member of a team, pay or receive an invoice through ABX, or simply visit our website.

Who we are and how to contact us

- **Company:** HAYAT GORDEEV HOLDINGS EUROPE LTD, a company registered in England and Wales with company number 17229457. Registered office: 35 Ballards Lane, London N3 1XW, United Kingdom. We operate ABX Wallet at www.abxwallet.com.
- **Privacy contact:** aziz@abacustechnologies.co. Please use this address for any question or request about this policy or your personal data.
- **ICO registration:** we are registered with the Information Commissioner's Office, reference ZC174004.
- **Law:** this policy is governed by the laws of England and Wales, and we follow the UK GDPR and the Data Protection Act 2018.

The short version

- ABX Wallet is a service for businesses. We do not hold your funds: for companies in Nigeria and Kenya, your company's USDT is held by Busha, an independent provider, and we pass your payment, top-up and cash-out instructions to it. We may need to verify your business and share the results with Busha (section 4.4).
- We use personal data to run the Service, keep it secure and meet our legal duties, including sanctions screening.
- We do not sell personal data and we do not use it for advertising.
- The invoices our business customers put into ABX belong to them. For the people named in those invoices, we mostly act on our customer's instructions, but we also use invoice details for our own purposes, such as preventing fraud and improving ABX (section 3). We never use them to train AI models.
- Your company's USDT balance is recorded by Busha. Supplier payments and payments of sent invoices are public Tron transfers: anyone can see them, and they cannot be deleted (section 5).
- You have rights over your personal data, and you can complain to us or to the ICO (section 11).

1. WHAT WE COLLECT

The personal data we hold depends on how you use ABX. Words such as "Admin", "Payer" and "Payment Page" have the meanings given in our Terms of Service.

1.1 Account details

- Your email address, full name, password (stored only as a one-way hash, never in readable form), sign-up date, last sign-in and account status.
- Which version of our Terms of Service and Data Processing Agreement you accepted, which version of this policy you acknowledged, and when.
- Details of your business: its name, billing settings, account status (including whether the account is on hold following sanctions screening) and, if it closes its account, the closure date.

- Sign-in security data: verified email addresses, two-factor authentication settings and recovery codes, and your sign-in sessions.

1.2 Your team

- Which businesses you belong to and your role (Admin, Manager or Bookkeeper).
- Invitations: the email address and role of the person invited, the invitation link and its expiry, and when the invitation was accepted or withdrawn.

1.3 Invoices you upload or enter

- Everything we read from each invoice: invoice number, issue and due dates, the issuer's and bill-to names, addresses and contact details (including the names of contact people, phone numbers and email addresses), tax, VAT and company registration numbers, line items, quantities and prices, tax amounts, bank and other payment details, payment terms and references, a short summary, the payment address, network and coin, and any other information on the document.
- Both amounts where an invoice states them: the total in the invoice's own currency (for example, SGD 5,835.86) and the amount the supplier asks to be paid in a stablecoin (for example, 4,132.55 USDT). We show both and do not convert between them.
- The raw output of the reading service (with confidence scores and page references), the original values, your corrections and sign-offs, and an edit history showing which field changed, from what, to what, by whom and when.
- The file name, size and a digital fingerprint (hash) of each file. The PDF itself is held in Abacus Docs, our document-reading service. If you enter an invoice manually, we keep the PDF ourselves.
- We use these details to provide the Service to the business that put the invoice into ABX and also, as a controller, for our own purposes described in section 3.

1.4 Invoices you send

- Your sender profile: business name, address, email, registration number, payment terms and logo.
- Each invoice you send: its number and dates, your name and your customer's name, addresses and email addresses, line items, notes, total (in US dollars), the address to be paid (the business's Busha deposit address), the PDF and the link to its Payment Page.
- Payments made on those invoices: the amount, the wallet addresses, the transaction hash and status and, where the payer is another ABX customer, which business paid.
- "Bill me via ABX" requests: the supplier's email address, the status of the request, its link and the relevant dates.

1.5 USDT account and payments

- Your company's USDT account (available to companies in Nigeria and Kenya): when a company opens it on the Account page, its country, phone number, address and city, and its cash-out destination (a Nigerian bank account number or a Kenyan M-Pesa phone number). We also store the Busha customer id, the account status, the company's deposit address and the ids of each transfer.
- **Verification information**, if we ask for it before or after a company opens its USDT account: incorporation documents, proof of address, board resolutions, bank statements and information about the source of funds; the names, identity documents and proof of address of directors, beneficial owners and users; and the results of our checks.

- Your approved suppliers (names and notes) and the wallet addresses approved for them: who approved each address, when, and from which invoice. If you dismiss a look-alike address warning, we record the reason you give.
- Each payment: the amount, coin and network, the sending and receiving addresses, the transaction hash, status and confirmations, any ABX fee details, what our payee check found and whether you confirmed a warning, and when the receipt email was sent.

1.6 Compliance records

- The sanctions lists we download (the UK, UN, EU and US OFAC lists), which contain names, aliases, countries, identifiers and wallet addresses.
- Screening results: who or what was checked, the outcome, and which lists and list versions matched; review cases and the decisions of our reviewers; and screening settings, including the email addresses that receive alerts.

1.7 Activity records

- An activity log for each business: what was done, by whom, to what, with a short description.
- When a member of our staff opens a customer record, we log it and show it to the customer as "ABX staff".

1.8 Technical data and the address checker

- Your IP address, browser and device information, and our server logs.
- If you use our public address checker, the Tron address you enter. We read that address's public history to give you a result. We do not store the address or the result, but the blockchain data provider we use may keep them in its own logs.

1.9 Demo uploads

- If you try the demo on our website without an account, the invoice PDF you upload and what we read from it. Demo uploads are not linked to any account and are deleted after about 60 minutes.

1.10 Adding money and cashing out

- **Top-ups and cash-outs:** when an Admin adds naira by bank transfer (Nigeria) or Kenyan shillings by M-Pesa (Kenya), or cashes out, the amount, the currency, the cash-out destination used, the status and the Busha transfer id.

1.11 Messages to us

- If you email us or ask for support, your contact details and what you tell us.

1.12 People without an ABX account

- **Payers** who open a Payment Page: their email address (as given on the invoice), the wallet address they pay from and the transaction details.
- **Suppliers** who receive a "bill me via ABX" request: their email address.
- **People named in invoices**, such as suppliers, customers and their staff: the details on the invoice. Section 3 explains our role for this information.

What we do not collect

We do not hold customer funds or the private keys to any company's USDT account: Busha holds them. Apart from manually entered invoices, invoice PDFs are not stored in our own database; they are held in Abacus Docs.

2. WHY WE USE IT, AND OUR LEGAL BASIS

We may only use personal data where the law gives us a reason (a "legal basis"). The table shows what we use your data for and the legal basis we rely on.

What we use it for	Data used	Legal basis
Providing ABX Wallet: creating and running accounts, sign-in and two-factor authentication, teams and roles, reading invoices, passing payment, top-up and cash-out instructions to Busha, sending invoices and receipts	Account, team, invoice, USDT account and payment data; security data	Contract, where you are our customer. Where you use ABX for the business you work for, our legitimate interest in providing the Service that business has signed up for.
Billing our customers for their subscription	Business and billing details; account email addresses	Contract; legitimate interests
Keeping the Service secure, preventing fraud and abuse, and investigating incidents	Technical data, activity records, staff access logs	Legitimate interests
Using invoice details for our own purposes: detecting and preventing fraud and changed or look-alike payment details across all ABX customers, analysing, testing and improving ABX and Abacus Docs, and creating anonymised statistics (section 3)	Invoice data, including the names, contact details, bank details and wallet addresses of suppliers, customers and Payers	Legitimate interests (preventing fraud and protecting our customers; improving our service)
Sanctions screening and related reviews (section 6)	Names and wallet addresses; screening results	Legal obligation (UK sanctions law); legitimate interests (screening against the UN, EU and US lists and frozen-address lists, and protecting ABX and its customers)
Keeping records we must keep, and dealing with authorities	Payment and screening records	Legal obligation; legitimate interests
The public address checker and the demo	Addresses entered; demo uploads; technical data	Legitimate interests (letting visitors try our checks)
Opening and running your company's USDT account with Busha: passing your details, amounts, cash-out destination and supplier Tron addresses to Busha (section 4.4)	Business name, email, country, phone, address and city; amounts; cash-out destination; supplier Tron addresses; verification information Busha asks for	Contract, where you are our customer; otherwise legitimate interests (providing the Service your business has signed up for)
Verifying businesses and the people behind them before and while they use the USDT account, keeping records of our checks, and sharing them with Busha	Verification information; account details; screening results	Legitimate interests (preventing financial crime and meeting our obligations to Busha); legal obligation, where the law requires these checks
Answering your messages	Contact details and messages	Legitimate interests
Establishing, exercising or defending legal claims	Any relevant data	Legitimate interests; legal obligation

Where we rely on legitimate interests, we have balanced our interests against yours, and you can object (section 11). If we ever need your consent for something, we will ask for it clearly and you can withdraw it at any time.

We do not sell personal data, and we do not use it for advertising.

3. OTHER PEOPLE'S DATA IN YOUR INVOICES

Invoices contain information about people: suppliers and their staff, our customer's own customers and Payers, and their staff. When a business customer uploads, enters or sends invoices through ABX,

that business is the **controller** of this information, and we are its **processor** when we use it to provide the Service to that business. This means:

- we use the information only to provide the Service to that business, on its instructions, under our Data Processing Agreement with it (the "DPA"), published at www.abxwallet.com/dpa;
- the business is responsible for having a lawful reason to use the information and for telling the people concerned; and
- when we email an invoice, receipt or "bill me via ABX" request on a customer's behalf, it comes from our email address and shows the customer's name followed by "via ABX Wallet".

We act as a controller, not a processor, when we screen names and wallet addresses against sanctions lists, for technical data such as the IP address of a device that opens a Payment Page, and when we use invoice data for our own purposes, as described below.

Our own use of invoice data. We capture all the details on the invoices put into ABX, and we also use them, as a controller, to:

- detect and prevent fraud, such as an invoice whose payment details have been changed or imitate a real supplier's, including by keeping records of the payee names, bank details and wallet addresses we see across all our customers so that we can warn any customer;
- analyse, test and improve ABX and Abacus Docs, including checking how accurately invoices are read (our staff may look at samples of invoices to do this); and
- create anonymised or aggregated statistics, which do not identify any business or person.

We rely on our legitimate interests in preventing fraud, protecting our customers and improving our service. We do not use invoice data to train AI models, we do not sell it or use it for advertising, and we do not show one customer's invoices to another, except as ABX digital invoices (section 4.5). A warning may tell a customer that payment details do not match details we have seen elsewhere, without saying where. You can object to this use (section 11).

If you are named in someone else's invoice, section 11 explains how to contact us.

4. WHO WE SHARE DATA WITH

Each customer's data is kept separate from every other customer's data. We share personal data only with the people and organisations below.

4.1 Service providers that process data for us

Provider	What it does	Where
Google Cloud Platform (Google)	Hosting and storage of the Service and all customer data, including for Abacus Docs; AI processing for reading invoices, using Google's Gemini models	United Kingdom or the Netherlands
Mailgun (Mailgun Technologies, Inc.)	Sending our emails: invoices, receipts, notifications, verification emails and invitations	European Union (EU region)

Abacus Docs, the service that reads uploaded invoices, is our own document-reading service and is operated by us. It runs on Google Cloud Platform in the United Kingdom or the Netherlands.

Google Cloud Platform and Mailgun act on our instructions. For invoice data, they are the sub-processors listed in the DPA.

4.2 Blockchain data providers

To check payments, read balances, check Tether's list of frozen USDT addresses and look for look-alike addresses, we send wallet addresses and transaction identifiers to **TronGrid**, a public blockchain node and data service for the Tron network. TronGrid is a globally distributed service that we do not control.

We send it only wallet addresses and transaction identifiers, which are public blockchain data. It acts independently of us, and its own privacy terms apply.

4.3 Sanctions screening

We download the UK, UN, EU and US OFAC sanctions lists; we do not send any personal data to the bodies that publish them. When it is switched on, we also send wallet addresses to **Chainalysis**, through its public sanctions service, to check whether an address is sanctioned. Chainalysis is a globally distributed service that we do not control. We send it only wallet addresses, which are public blockchain data. It acts independently of us, and its own privacy terms apply.

4.4 Busha

Busha (Busha Digital Limited, a company incorporated in Nigeria, and its affiliates) holds the USDT of companies in Nigeria and Kenya and converts naira and Kenyan shillings into and out of USDT. The service is powered by Busha, a company that holds an Approval-in-Principle from the Securities and Exchange Commission (SEC) of Nigeria. When a company opens its USDT account, adds money, cashes out or pays a supplier, we send Busha the business name, email address, country, phone number, address and city, the amounts, the cash-out destination (a Nigerian bank account number or a Kenyan M-Pesa phone number) and the supplier's Tron address, together with any verification information Busha asks for. Busha may also collect other details it needs directly. Busha is an independent controller of this data, subject to Nigeria's data protection law, and its own privacy notice, at www.busha.io/privacy-policy, explains how it uses it. Busha is based in Nigeria and may transfer data to its affiliates and service providers in other countries (section 7).

4.5 Other ABX customers

If you pay an invoice issued by another ABX customer, or another ABX customer pays yours, a copy of the invoice appears in both accounts as an ABX digital invoice. A Payer who opens a Payment Page sees the invoice they have been sent.

4.6 Google Fonts and wallet apps

- Our website loads fonts from Google Fonts. Your browser connects to Google directly to do this, so Google receives your IP address.
- Business users do not connect wallet apps to ABX. Only someone paying a sent invoice through its Payment Page may pay from their own Tron wallet app, which runs in their own browser or phone. Wallet apps are not our service providers, and their own terms apply.

4.7 Authorities, advisers and a buyer of our business

- The police, regulators, courts and sanctions authorities, where the law requires or allows us to share data.
- Our professional advisers, insurers and auditors, who must keep it confidential.
- A buyer or successor, if our business is sold or reorganised.

5. BLOCKCHAINS ARE PUBLIC AND PERMANENT

Your company's USDT balance is a record in Busha's own systems (its ledger), not on a public blockchain, and Busha's privacy notice applies to it. Supplier payments, and payments made to a sent invoice, are transfers on the public Tron blockchain. ABX supports only the Tron network; Ethereum and Solana are switched off. Anyone can see the wallet addresses, amounts and times of these transfers, and the records are permanent. Neither we nor anyone else can change or delete them. We do not control any blockchain.

6. SANCTIONS SCREENING AND AUTOMATED DECISIONS

We must not let ABX be used to deal with sanctioned people or addresses. We therefore screen names and wallet addresses against sanctions lists and lists of frozen addresses:

- at sign-up;
- when a wallet or payee is added or changed;
- when a payment is set up, and again when it is confirmed; and
- every day after that.

If a wallet address is on a sanctions list or a frozen-address list, ABX automatically blocks payments to it. Possible matches, such as a similar name, are always reviewed by a person before we decide what to do. As a result of screening we may hold a payment, invoice or registration, or hold, suspend or close an account. We may also report matters to the authorities where the law requires or allows, and to Busha where our agreement with it requires. The law sometimes prevents us from explaining why we have taken a decision.

If a decision based only on automated processing has a significant effect on you, you can ask us for information about it, give us your point of view, ask for a person to review it and challenge it. To challenge any screening decision, email aziz@abacustechnologies.co with the details, and a person will review it.

7. INTERNATIONAL TRANSFERS

We are based in the United Kingdom. Our sub-processors process personal data only in these places:

Provider	Location
Google Cloud Platform	United Kingdom or the Netherlands
Mailgun	European Union (EU region)

Transfers from the United Kingdom to the Netherlands and the rest of the European Union are covered by UK adequacy regulations, which recognise the EU's data protection standards. Abacus Docs, our own document-reading service, runs on Google Cloud Platform in the same places.

Busha is not our sub-processor: it is an independent controller (section 4.4). It is based in Nigeria, operates in Nigeria and Kenya, and may transfer data to its affiliates and service providers in other countries. Neither Nigeria nor Kenya is covered by UK adequacy regulations, so we send data to Busha only in accordance with UK data protection law on international transfers. You can ask us for details of the safeguards we rely on at aziz@abacustechnologies.co.

The blockchain data provider (TronGrid) and Chainalysis described in sections 4.2 and 4.3 are globally distributed services that we do not control, and we do not control where they process data. We send them only wallet addresses and transaction identifiers, which are already public on the blockchain.

8. HOW LONG WE KEEP DATA

Data	How long we keep it
Your account, invoices, USDT account details and other customer data	While the account is open. When the account closes or the Terms of Service end, we delete it or make it inaccessible, including from backups and archives, within 360 days, except records the law requires us to keep or that are described below.
Invoice data we use for our own purposes (section 3)	Fraud-prevention records (payee names, bank details and wallet addresses): up to five years after we last see them. Data used to analyse and improve ABX: as for other customer data. Anonymised statistics: kept indefinitely, as they do not identify anyone.
Sanctions screening records and payment records	At least five years.

Data	How long we keep it
Verification information and records of our checks	At least five years after the business's account closes.
Demo uploads	Deleted after about 60 minutes.
Technical logs	365 days.
Address checker	We do not store the address you enter or the result. They may appear in the data provider's logs.
Data held by Busha	Busha keeps its own records under its own privacy notice.
Messages to us (support messages and emails)	365 days.
Blockchain data	Cannot be deleted. It is public and permanent, and we do not control it.

If you delete an invoice, we delete the uploaded file and the copy held in Abacus Docs, unless a sent or paid payment is attached to it or we must keep it. Before closing its account, a business can ask us for an export of its records as a ZIP file. The export does not include our own sanctions screening records, password hashes or other customers' data.

9. COOKIES

We use only the cookies the Service needs to work: a sign-in session cookie and a security cookie that protects forms against misuse. Because these cookies are strictly necessary, we do not ask for consent to use them. We do not use advertising or analytics cookies. Our website loads fonts from Google Fonts, so Google receives your IP address (section 4.6).

10. SECURITY

We protect personal data with measures that include:

- two-factor authentication, available to every user (it is optional, and we recommend turning it on), and passwords stored only as one-way hashes;
- encryption of customer data at rest;
- encrypted connections (HTTPS, with HSTS) and secure, HttpOnly and SameSite cookies;
- role-based access (only Admins can pay or cash out), and each business's data kept separate so that no customer can reach another's data;
- staff access to customer data only for specific reasons (a support request, a sanctions review, a security or fraud investigation, checking the accuracy of invoice reading, or a legal duty), limited to what is necessary, logged and shown to the customer as "ABX staff";
- an activity log of sensitive actions such as uploads, edits, payments, exports, team changes and closures;
- rate limits on public tools such as the demo and the address checker;
- never holding customer funds or the private keys to them: each company's USDT is held by Busha, and a payment is sent only when an Admin confirms it;
- never using customer data to train AI models; and
- an incident response process, handled by Hayat Gordeev Holdings Europe Ltd.

If a personal data breach affects you, we will tell you within 72 hours of discovering it. Where the law requires it, we will also notify the ICO.

No system is completely secure, so please keep your password, two-factor device and recovery codes safe, and tell us at once at aziz@abacustechnologies.co if you suspect misuse.

11. YOUR RIGHTS

Under UK data protection law you have the right to:

- ask for a copy of your personal data;
- ask us to correct data that is wrong or incomplete;
- ask us to delete your data;
- ask us to restrict how we use your data;
- object to our use of your data where we rely on legitimate interests;
- ask for your data in a portable format, where the law allows;
- ask for a person to review a decision based only on automated processing (section 6); and
- withdraw consent at any time, where we rely on it.

These rights have limits. For example, we may need to keep some records by law, such as payment and screening records. To use your rights, email aziz@abacustechnologies.co. We may ask you to prove your identity. We normally reply within one month, and there is usually no charge.

If you are named in someone else's invoice

If you are a supplier, customer or Payer of one of our business customers, or work for one, that business controls the data about you in its invoices, and we control our own uses of it described in section 3. You can still contact us at aziz@abacustechnologies.co. We will pass requests about invoice content to the business concerned and help it respond, and we will deal directly with anything we control, such as sanctions screening, technical data and our own uses of invoice data, including any objection to them.

Complaints

If you are unhappy with how we have used your personal data, please tell us first at aziz@abacustechnologies.co. We will acknowledge your complaint within 30 days and keep you informed until it is resolved. You also have the right to complain to the Information Commissioner's Office (ICO), the UK's data protection regulator: ico.org.uk.

12. AGE

ABX is a service for businesses. It is not for anyone under 18, and we do not knowingly collect personal data from anyone under 18.

13. CHANGES TO THIS POLICY

The version number and the date of the last update are shown at the top of this policy, and we keep copies of earlier versions. If we make a material change, we will tell account holders before it takes effect, by email or through the Service. When you sign up, and when we ask you to accept new versions of our Terms of Service and DPA, we ask you to acknowledge that you have read this policy. This policy is a notice: it is not part of our contract with you.