amdax

Privacy Statement

Amdax · Gustav Mahlerplein 49 · 1082 MS Amsterdam · The Netherlands
KVK: 74458477 · Telephone: +31 88 263 29 00 · Email: hello@amdax.com

01

Introduction

This Privacy Statement explains how Amdax B.V. ("Amdax," "we," "us," or "our") collects, uses, shares, and protects your personal data when you use our services, visit our website, or otherwise interact with us.

We are committed to processing your personal data in accordance with the General Data Protection Regulation (EU) 2016/679 ("GDPR") and other applicable data protection laws.

This Privacy Statement may be updated from time to time to reflect changes in our practices or legal requirements. The most recent version will always be available on our website. We will notify you by email of any material changes.

This Privacy Statement is published in multiple languages. In the event of any discrepancy between translations, the Dutch version shall prevail.

02

Data Controller

Amdax B.V., registered with the Dutch Chamber of Commerce under registration number 74458477, located at Gustav Mahlerplein 49, 1082 MS Amsterdam, the Netherlands, is responsible for the processing of your personal data as described in this Privacy Statement and acts as 'controller' under the GDPR.

If you have any questions about this Privacy Statement or wish to exercise your rights, you can contact us at hello@amdax.com.

03

What Personal Data We Collect

Personal Data means any information that identifies you, as a natural person, or could reasonably be used to identify you, such as your name, BSN-number or email address.

3.1 Personal Data we collect directly from you

When you open an account or use our services, we may collect the following categories of Personal Data directly from you:

- **Identification data**: full name, email address, phone number, postal address, government-issued identification documents (such as a passport or driver's license), date of birth, nationality;
- **Financial data**: bank account details, source of wealth, routing number;
- **Commercial data**: trading activity, deposits, withdrawals, account balances;
- **Blockchain data**: wallet addresses, transaction IDs, amounts, timestamps;
- **Customer support data**: onboarding forms, correspondence, customer support tickets;
- **Biometric data**: face scan for identity verification;
- **Company data** (where relevant): legal entity details, registry numbers, articles of association, proof of legal existence;
- **Socio-demographic data** (where relevant to the provision of the services or applicable legal requirements): employment status, marital status, dependents.
- **Contact request data** (when you use the contact form on our website): first and last name, email address, phone number, account type, the services you are interested in and your consent choices.

Certain personal data is required by law or necessary to enter into or perform a contract with you. Where this is the case, we will indicate this at the point of collection. If you do not provide the required data, we may be unable to open an account for you or provide some or all of our services.

3.2 Personal Data we collect automatically

When you interact with our platforms, we may automatically collect:

- **Online identifiers and device data**, such as IP address, browser, operating system, device attributes, and identifiers stored in cookies and similar technologies;
- **Usage data**, such as system activity, pages visited on Amdax, clickstream data, and, if you consent to analytics cookies, session recordings of how you use our website, such as clicks, scrolling and mouse movements, shown as recordings and heatmaps;
- **Geolocation data**, where required for due diligence or to strengthen security;

- **Marketing data**, such as communication preferences, subscription settings, opt-in data, interaction signals such as email opens or clicks, where relevant;
- **Social media data**, such as your engagement with Amdax accounts on platforms where you interact with us directly.

We collect part of this data through cookies and similar tracking technologies on our websites and apps (see section 3.4). We refer to our Cookie Statement, published at www.amdax.com/en/legal-compliance#cookie-statement, for more information about our use of cookies and similar technologies.

Furthermore, we may generate data about you based on your activity on our platform, including behavioral patterns, risk profiles, and transaction profiles, which help us meet our compliance, security, and fraud prevention obligations.

Personal Data provided during registration may be retained even if your registration is incomplete or abandoned.

3.3 Personal Data we collect from third parties

We may collect or verify your Personal Data from trusted third parties, including service providers, public sources, and regulators. This may include:

- **Identification data**, such as ID document validation;
- **Financial data**, such as bank account verification;
- **Blockchain data**, such as wallet address screening and transaction analysis;
- **Third-party verification data**, such as Chamber of Commerce (or any other relevant company register) registration data;
- **Sanctions and watchlist data**, such as PEP and sanctions screening results;
- **Affiliated persons' data**, such as joint account holders, transaction counterparties, referees.

3.4 Use of cookies

When you visit our website or use our platform, we use cookies and similar technologies. We use three categories:

Category	Purpose	Legal Basis
Necessary	Required for the website and platform to function (e.g. login sessions, security, storing your cookie choice, bot protection, support chat)	Performance of a contract (platform login) Legitimate interests (website security, support chat) Legal obligation (recording your cookie choice)
Analytics	Understand how visitors use our website, including session recordings and heatmaps and how clients use our platform.	Consent
Marketing	Measure and improve advertising campaigns and show you relevant ads on other platforms (see section 6)	Consent

When you first visit our website, a cookie banner lets you accept all cookies, reject all cookies or set your preferences. Until you make a choice, and if you reject all, we only use necessary cookies. You can change or withdraw your choice at any time via "Cookie preferences" at the bottom of our website. Our Cookie Statement lists each cookie on our website, its provider, its purpose and how long it is stored.

Please note that blocking necessary cookies in your browser may prevent you from using some or all features of the Amdax platform.

3.5 Children's data

We only collect and process Personal Data from minors with verified parental or legal guardian consent when a child account is opened. A child account can only be created if the parent or legal representative already holds an individual account with Amdax.

Parents or legal representatives retain access to the account until the child turns 18, at which point the child assumes full control.

3.6 Special categories of Personal Data and criminal data

We may process special categories of Personal Data, such as biometric data, as this is necessary for identification, authentication, and compliance purposes, on the basis of article 9(2)(g) GDPR (substantial public interest), read together with the Dutch GDPR

Implementation Act (UAVG) and the Dutch Money Laundering and Terrorist Financing (Prevention) Act (Wwft).

We may also process personal data relating to criminal offences (including information relevant to AML/KYC screening) where necessary to comply with our legal obligations under the applicable laws and regulations, such as the Dutch Money Laundering and Terrorist Financing (Prevention) Act (Wwft).

04

How We Use Your Personal Data

The Personal Data we collect is used to provide you with the best possible experience, protect you from fraud and misuse, and help us maintain and improve the Amdax services.

We may use your Personal Data to:

- **Provide our services**: we process your Personal Data to fulfill the terms of your agreement with us. For example, to facilitate fiat transfers to or from your account, we require your bank account details.
- **Comply with legal and regulatory obligations**: we process your Personal Data as required by applicable laws and regulations. For example, we have identity verification requirements to fulfill our obligations under anti-money laundering laws.
- **Protect the security and integrity of our services**: we may process your Personal Data to detect threats and ensure the security of our platform.
- **Provide you with customer support**: we may use your Personal Data when responding to your customer service inquiries.
- **Optimize and enhance our services**: we may use your Personal Data to improve our services, develop new features and enhance user experience.
- **Market our products and services**: with your consent, we may send you product updates, promotional materials, or marketing communications. You may withdraw your consent at any time by following the unsubscribe instructions in our communications.
- **Other business purposes**: we may use your Personal Data for additional purposes disclosed to you at the time of collection or with your consent.

The table below shows the main purposes for which we process Personal Data, the categories of data involved, and the legal basis we rely on. We prioritize the strongest bases such as legal obligations or contracts and only rely on legitimate interests or consent where appropriate.

This list is illustrative and may vary depending on the specific services you use.

Purpose	Personal Data	Legal Basis
Compliance with legal and regulatory obligations (e.g., AML/KYC, tax, financial rules)	Identification data; financial data; blockchain data; biometric data; company data; sanctions and watchlist data; third-party verification data; affiliated persons' data; socio-demographic data.	Legal obligation Performance of a contract
Providing and managing your account	Identification data; commercial data; financial data; customer support data.	Performance of a contract Legal obligation
Fraud prevention, security, and risk management	Identification data; online identifiers and device data; geolocation data; usage data; affiliated persons' data.	Legitimate interests Legal obligation
Customer support and service quality	Customer support data; survey data (feedback forms).	Performance of a contract Legitimate interests Consent (for optional surveys)
Handling your contact request	Contact request data.	Steps at your request before entering into a contract Consent (for marketing follow-up, where given)
Business operations and product improvement	Usage data; registration data; survey data; social media data (interactions with Amdax accounts); online identifiers and usage data from analytics cookies, including session recordings.	Legitimate interests Consent (where required, including analytics cookies)

Purpose	Personal Data	Legal Basis
Marketing and communications	Marketing data; social media data (engagement and interactions with Amdax accounts); online identifiers from marketing cookies, used for ad measurement and targeting.	Legitimate interests Consent (including marketing cookies)

05

How long we keep your personal data

We retain personal data only for as long as necessary for the purposes for which it was collected, to comply with our legal obligations, and to resolve disputes or enforce agreements. The exact retention periods of the various records maintained are outlined below:

Category of Personal Data	Retention Period
Client agreement and account data	5 years
AML/KYC and identity verification data	5 years
Transaction records	5 years
Customer support correspondence	5 years
Contact form copies in our website system	30 days
Marketing data	5 years
Cookie data and online identifiers	As set out per cookie in our Cookie Statement: from the end of the browser session up to 400 days

In some cases, we may be required to retain data for longer, for example when directed by a supervisory authority or in connection with a legal claim. Once data is no longer required, it is securely deleted or anonymized. Anonymized data may be retained indefinitely.

06

Automated Decision-Making and Profiling

We use verification tools to confirm the validity of identity documents, ensure consistency between submitted data, and prevent the use of our services by individuals who do not meet the applicable eligibility requirements. Where automated checks raise concerns, applications are always subject to manual review by our KYC onboarding team. If your identity document or bank account is not approved, you can request an additional manual review, share your point of view, and/or contest the decision by contacting our Customer Support.

Additionally, we continuously monitor whether new information may affect a client's risk profile or transaction activity, and whether behavior remains consistent with the information we hold. Automated tools may update a client's risk classification and can trigger additional checks on certain transactions. Depending on the outcome, transactions may be reviewed by the compliance team either before or after execution. In some cases, updated risk assessments may also lead to more frequent reviews of account details. You can contact our Customer Support if you wish to request an additional review or provide further clarification regarding a transaction.

If you consent to marketing cookies, Google, Meta and LinkedIn may each combine information about your visit to our website with other information they hold about you, to build a profile of your interests and show you targeted advertising, including ads for Amdax. We use this to measure our campaigns and reach relevant audiences. This profiling does not lead to decisions that have legal effects for you or affect you in a similarly significant way. You can withdraw your consent at any time via "Cookie preferences" on our website.

07

How We Share Your Personal Data

We will not share your Personal Data with third parties, except as described below:

Service Providers and other third parties: we may share your Personal Data with third-party service providers for business or commercial purposes, such as identity verification, fraud detection and prevention, customer screening, security threat detection, payment processing, data analytics, information technology, advertising, marketing, network infrastructure, and storage.

When we use the services of such a third-party service provider that processes your Personal Data on our behalf and acts as a data processor, data processing agreements are put in place in accordance with applicable data protection laws to ensure the correct and safe processing of your Personal Data and to ensure compliance with international data transfer restrictions.

We may share your Personal Data with third parties who process Personal Data for their own purposes (and do not qualify as processors but as 'controllers') in limited circumstances.

Cookie and tag providers: if you accept analytics or marketing cookies, data about your visit to our website is shared with the providers of those cookies: Google (Google Analytics, Google Ads, YouTube), Microsoft (Clarity), HubSpot, LinkedIn (Insight Tag) and Meta (Meta Pixel, loaded through HubSpot). Zendesk and Cloudflare receive data through necessary cookies for our support chat and bot protection. For the collection and transmission of event data via the Google Ads tags, the Meta Pixel and the LinkedIn Insight Tag, Amdax acts as joint controller together with Google, Meta and LinkedIn respectively. Each of these providers acts as an independent controller for its own further use of that data. The essence of these joint-controller arrangements, including the applicable terms (such as the Meta Controller Addendum and the LinkedIn DPA), is set out in our Cookie Statement. Our Cookie Statement lists the providers per cookie.

Contact form: when you use the contact form on our website, the data you enter is sent directly to HubSpot, which we use as our customer relationship management system. HubSpot processes this data on our behalf as our processor and under our instructions. The contact form does not place HubSpot cookies in your browser.

Compliance with legal and regulatory obligations: we may use your Personal Data to comply with a range of legal obligations and statutory requirements, including banking and financial regulations that oblige us to comply with our regulatory obligations, such as:

- Public authorities, regulators and supervisory bodies such as the Authority for Financial Markets (AFM) in the Netherlands.
- Tax authorities may require us to report customer assets or other Personal Data such as your name and contact details and other data about your organization. For this purpose, we may process your identification data such as BSN number, tax identification number or any other national identifier in accordance with applicable local law.
- Judicial/investigative authorities such as the police, public prosecutors, courts and arbitration/mediation bodies at their express and legal request.

Corporate Transactions: we may disclose Personal Data in the event of a proposed or consummated merger, acquisition, reorganization, asset sale, or similar corporate transaction, or in the event of bankruptcy or dissolution.

Professional Advisors: we may share your Personal Data with our professional advisors, including legal, accounting, or other consulting services for purposes of audits, business purposes or to comply with our legal obligations. Your data will be processed by persons working for our behalf on a 'need-to-know' basis, solely for the purposes specified in this Privacy Statement.

Consent: we may share or disclose your Personal Data with your consent, such as upon exercising your right to data portability.

If we decide to modify the purpose for which your Personal Data is collected and used, we will amend this Privacy Statement.

08

International Data Transfers

As Amdax may work with various processors, your data may be transferred to and processed in countries outside the Netherlands. Within the European Economic Area (EEA), data protection standards are equivalent and transfers are permitted subject to applicable legal requirements.

If Personal Data is transferred to a country outside the EEA that does not provide an adequate level of protection under the applicable law and/or not covered by an adequacy decision of the European Commission, we implement appropriate safeguards including the use of standard contractual clauses approved by the European Commission to protect your Personal Data.

Several of our providers, including Google, Microsoft, HubSpot, Zendesk, LinkedIn and Meta, are based in the United States or may process data there. Where a provider is certified under the EU-U.S. Data Privacy Framework, the transfer is based on the adequacy decision of the European Commission of 10 July 2023. Where it is not, we use standard contractual clauses.

09

How We Protect Your Personal Data

We apply strict security standards and use a combination of technical, organizational, and procedural measures to protect your Personal Data from unauthorized access, alteration, disclosure, or destruction.

These measures include:

- **Encryption**: Personal Data is protected through encryption both in transit and at rest.
- **Authentication and identity verification**: two-factor authentication is required for all user sessions, and we may request additional identity verification to protect accounts against unauthorized access.
- **Security reviews**: we conduct periodic reviews and assessments to identify and address potential vulnerabilities.
- **Access controls**: access to Personal Data is restricted to authorized personnel only, based on role and necessity. We apply contractual confidentiality obligations for employees, contractors, and agents who process such data.
- **Physical safeguards**: Personal Data is stored in secure facilities with controlled access, alongside electronic and procedural safeguards, to protect against physical tampering or theft.
- **System safeguards**: we implement measures to limit shared access to customer data and regularly review access rights in shared platforms ensuring that only those with a business need retain access.

While we take these measures seriously, no system is entirely immune to security risks. We therefore encourage you to protect your own account by using a strong and unique password, signing out on shared devices, and staying vigilant for suspicious activity.

10

Your Data Subject Rights

You have the following privacy rights with regards to our processing of your Personal Data:

- **Right of access**: you have the right to request confirmation if we process your Personal Data and obtain a copy of the data we hold.

- **Right to rectify your Personal Data**: you have the right to request correction of inaccurate or incomplete Personal Data about you. Such requests can be submitted through your My Amdax account.
- **Right to delete your Personal Data**: you have the right, in some cases, to request deletion of your Personal Data. In some cases, we may be legally required to retain your data.
- **Right to restrict our processing**: you have the right to request limitation of data use in certain circumstances such as when contesting accuracy.
- **Right to data portability**: you have the right, in certain circumstances, to obtain your Personal Data in a structured, commonly used and machine-readable format or transfer it to another party where technically feasible.
- **Right to object**: you have the right to object to our processing of your Personal Data, except where we demonstrate compelling legal grounds.
- **Right not to be subject to solely automated decisions**: you have the right to request human intervention in automated decision-making processes that significantly affect you, express your point of view, and contest the outcome.
- **Right to withdraw consent**: you have the right to withdraw your consent at any time where processing is based on consent, including your consent for cookies via "Cookie preferences" on our website. This will not affect prior lawful processing.
- **Right to lodge a complaint:** you have the right to file a complaint with your local supervisory authority or with the Dutch Data Protection Authority via autoriteitpersoonsgegevens.nl, if you are concerned about how we have processed your Personal Data.
- **Right to object to direct marketing**: you may opt out of these communications at any time by using the unsubscribe links provided in them, or by contacting us directly.

You can exercise your rights by contacting us using the details provided in Section 11 below.

We may need to verify your identity before accommodating your request. After the verification, we will proceed with the relevant procedure. We will respond as quickly as possible, but in any event no later than one month after the receipt of your request. If we need additional time to process your request, we will inform you accordingly.

Please note that the above rights are not absolute and may be subject to limitations or exceptions under applicable laws. If we are unable to fulfill a request in relation to your rights, we will inform you of the reasons why we cannot accommodate your request.

11

Contact

If you have any questions regarding this Privacy Statement, our processing of your Personal Data, or if you wish to exercise one of your data subject rights, you may contact us at hello@amdax.com or by post at:

Amdax B.V.
Gustav Mahlerplein 49
1082 MS Amsterdam
The Netherlands

If you are not satisfied with how we have handled your Personal Data, you may lodge a complaint with the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) at autoriteitpersoonsgegevens.nl.

If you reside in another EU member state, you may also contact your local data protection supervisory authority.