



Privacy Policy

Version: January 2026



CONTENTS

1.	ABOUT US.....	3
2.	OUR COMMITMENT AND THE LAW WE FOLLOW	3
3.	SCOPE OF THIS POLICY	3
4.	PERSONAL DATA WE COLLECT	4
5.	WHERE WE OBTAIN PERSONAL DATA.....	4
6.	HOW WE USE PERSONAL DATA AND OUR LEGAL BASES	5
7.	AUTOMATED DECISION-MAKING AND PROFILING	6
8.	WHO WE SHARE PERSONAL DATA WITH	6
9.	INTERNATIONAL TRANSFERS	7
10.	RECORDING OF COMMUNICATIONS	7
11.	HOW LONG WE KEEP PERSONAL DATA	7
12.	YOUR RIGHTS	8
13.	SECURITY OF PERSONAL DATA	8
14.	PERSONAL DATA BREACHES	9
15.	SOCIAL NETWORKS	9
16.	COOKIES.....	9
17.	CHANGES TO THIS POLICY.....	9
18.	COMPLAINTS.....	9



1. ABOUT US

1.1. NAGA X Ltd ("NAGA X", the "Company", "we", "us" or "our") is a company registered in the Republic of Cyprus under number HE 424746, with its registered office at Agias Zonis 11, 3027 Limassol, Cyprus. The Company is authorised by the Cyprus Securities and Exchange Commission ("CySEC") as a Crypto-Asset Service Provider ("CASP") under Regulation (EU) 2023/1114 on markets in crypto-assets ("MiCA"), CASP number 009/23.

1.2. NAGA X is part of the group of companies of The NAGA Group AG (the "NAGA Group"). For the purposes of this Privacy Policy (the "Policy"), NAGA X is the controller of your personal data, which means that we decide why and how your personal data is processed.

1.3. We have appointed a Data Protection Officer ("DPO"). You can contact the DPO about any matter relating to this Policy or your personal data:

Item	Details
Entity	NAGA X Ltd
Contact person	Data Protection Officer
Email	dpo@nagax.com
Postal address	Agias Zonis 11, 3027 Limassol, Cyprus

2. OUR COMMITMENT AND THE LAW WE FOLLOW

2.1. We are committed to protecting your personal data and to processing it lawfully, fairly and transparently. We process personal data in accordance with Regulation (EU) 2016/679 (the "GDPR"), the Cyprus Law on the Protection of Natural Persons with regard to the Processing of Personal Data and the Free Movement of such Data (Law 125(I)/2018), and the other laws that apply to us as a CASP, including MiCA, Regulation (EU) 2023/1113 (the "Transfer of Funds Regulation" or "Travel Rule") and the Cyprus Prevention and Suppression of Money Laundering and Terrorist Financing Law (Law 188(I)/2007).

3. SCOPE OF THIS POLICY

3.1. This Policy explains how we collect, use, share and protect personal data when you visit our website at <https://nagax.com/eu> and its subdomains (the "Website"), use the NAGA X platform and mobile applications (the "Platform"), interact with us on social networks, or receive our crypto-asset services.

3.2. This Policy applies to our clients and prospective clients, visitors to the Website and Platform, and the representatives, directors, shareholders and beneficial owners of corporate clients.

3.3. Our services are not intended for persons under 18 years of age. We do not knowingly collect personal data from minors. If you believe a minor has provided us with personal data, please contact the DPO so that we can delete it.

4. PERSONAL DATA WE COLLECT

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

Category	Examples
Identity data	Full name, date and place of birth, nationality, gender, national identity or passport number, copies of identity documents.



Category	Examples
Contact data	Residential address, proof of address, email address, telephone number.
Verification data	Photographs and video taken during identity verification (including liveness checks) and the results of those checks.
Financial profile	Occupation and employer, annual income, net worth, source of funds and source of wealth, expected account activity and supporting documents.
Tax data	Tax residence and tax identification number.
Suitability data	Knowledge and experience of crypto-assets, investment objectives, risk tolerance and ability to bear losses, collected where you use our copy-trading portfolio management service.
Account and transaction data	Account number and username, orders, exchanges, deposits, withdrawals, balances, statements, and the date, time, amount, price and crypto-asset of each transaction.
Crypto-asset transfer data	Distributed ledger addresses, transaction hashes, originator and beneficiary information required by the Travel Rule, evidence of ownership of self-hosted wallets, and the results of blockchain analytics on wallets and transactions.
Payment data	Bank account details (such as IBAN) and, for cards, only the last four digits, expiry date and cardholder name.
Screening data	Results of sanctions, politically exposed person ("PEP") and adverse media screening.
Communications data	Recordings of telephone calls, chat and email correspondence, complaints and survey responses.
Technical and usage data	IP address, approximate location derived from IP address, device and browser information, log-in records, and how you use the Website and Platform (see our Cookies Policy).
Marketing data	Your marketing and communication preferences and your responses to our communications.

4.2. Some verification data, such as facial images processed to confirm that you are the person shown in your identity document, may be biometric data and therefore a special category of personal data. We process it only where permitted by the GDPR and Applicable Law, and only for identity verification and fraud prevention.

4.3. Where we need personal data to comply with the law or to enter into a contract with you and you do not provide it, we may be unable to open your account or provide our services.

5. WHERE WE OBTAIN PERSONAL DATA

5.1. We collect most personal data directly from you, for example when you register, complete our questionnaires, upload documents, place orders or contact us.

5.2. We also obtain personal data from:

- identity verification and onboarding service providers;
- sanctions, PEP and adverse media screening databases;
- blockchain analytics providers;



- other CASPs that send or receive crypto-asset transfers to or from your account, as required by the Travel Rule;
- banks, electronic money institutions and payment service providers that process your deposits and withdrawals;
- other NAGA Group companies, where you are also their client and the law allows;
- introducers and affiliate partners who refer you to us;
- public registers, official sources and publicly available information, including media; and
- analytics and advertising providers (see our Cookies Policy).

6. HOW WE USE PERSONAL DATA AND OUR LEGAL BASES

6.1. We use personal data only where we have a legal basis under the GDPR. The main purposes and legal bases are:

Purpose	Legal basis
Opening and managing your account, and providing custody, exchange, order execution and transmission, transfer and copy-trading services	Performance of a contract with you, and taking steps at your request before entering into a contract.
Identity verification, customer due diligence, sanctions and PEP screening, transaction monitoring and reporting suspicious activity	Legal obligation under Law 188(I)/2007, CySEC directives and EU sanctions law.
Collecting and exchanging Travel Rule information and verifying ownership of self-hosted wallets	Legal obligation under Regulation (EU) 2023/1113.
Assessing suitability before providing copy-trading portfolio management	Legal obligation under MiCA.
Keeping records of services, orders, transactions and communications	Legal obligation under MiCA and Law 188(I)/2007.
Reporting information on crypto-asset transactions and tax residence to tax authorities	Legal obligation under applicable tax law, including the rules implementing Directive (EU) 2023/2226 ("DAC8").
Handling complaints and responding to regulators and authorities	Legal obligation and legitimate interests.
Preventing fraud, protecting accounts and keeping the Website and Platform secure	Legitimate interests (protecting our clients and our business) and legal obligation.
Establishing, exercising or defending legal claims	Legitimate interests.
Improving our services, analysing how they are used and producing aggregated statistics	Legitimate interests; consent where required for cookies.
Sending marketing communications about our products and services	Consent, which you can withdraw at any time.
Processing biometric data during identity verification	Explicit consent, or substantial public interest in preventing fraud and money laundering as permitted by law.



6.2. We will not use personal data that we keep solely to meet our record-keeping obligations for other purposes, such as marketing.

6.3. Where we rely on legitimate interests, we balance our interests against your rights and freedoms. You can ask the DPO for more information about this assessment.

7. AUTOMATED DECISION-MAKING AND PROFILING

7.1. We use automated tools to support decisions that are required to comply with the law and to protect our clients, in particular to:

- verify your identity and documents during onboarding;
- screen you against sanctions and PEP lists;
- assign and review your money laundering risk rating;
- monitor transactions and assess the risk of crypto-asset transfers using blockchain analytics; and
- assess whether our copy-trading portfolio management service is suitable for you.

7.2. Outcomes that significantly affect you, such as refusing to open an account or rejecting a transfer, are reviewed by our staff. You have the right to request human review, to express your point of view and to contest a decision made solely by automated means (see section 12).

8. WHO WE SHARE PERSONAL DATA WITH

8.1. We share personal data only where necessary for the purposes described in section 6, and only with:

Recipient	Why we share
Other NAGA Group companies	To provide shared support, technology and compliance functions, and to prevent financial crime, where permitted by law.
Identity verification, screening and blockchain analytics providers	To verify your identity, screen for sanctions and PEPs, and assess the risk of crypto-asset transfers.
Travel Rule service providers and counterparty CASPs	To transmit and receive originator and beneficiary information when you send or receive crypto-assets.
Custody technology provider	To operate the wallet infrastructure in which we safeguard crypto-assets.
Liquidity providers	To execute or transmit your orders. We share only the information needed for this purpose.
Banks, electronic money institutions and payment service providers	To process deposits and withdrawals of funds and to safeguard client funds.
IT, cloud hosting, data storage, customer support and communications providers	To operate the Website and Platform, store data securely, and communicate with you.
Auditors, professional advisers and insurers	To meet our audit, legal and insurance requirements.
Regulators and public authorities	For example CySEC, the Unit for Combating Money Laundering (MOKAS), tax authorities, courts and law enforcement, where required by law.



Recipient	Why we share
A buyer or successor of our business	In connection with a sale, merger or restructuring, subject to confidentiality obligations.

8.2. Our service providers act as processors on our instructions and under written contracts that require them to protect your personal data and not to use it for their own purposes. Some recipients, such as banks, payment service providers and counterparty CASPs, act as independent controllers and process your personal data under their own privacy notices.

8.3. We do not sell your personal data, and we do not share it with third parties for them to send you their own marketing without your consent.

9. INTERNATIONAL TRANSFERS

9.1. Some of our service providers are located, or store data, outside the European Economic Area ("EEA"). We transfer personal data outside the EEA only where:

- the European Commission has decided that the destination country provides an adequate level of protection (for example, the United Kingdom);
- the recipient in the United States is certified under the EU-U.S. Data Privacy Framework; or
- we have put in place appropriate safeguards, such as the European Commission's Standard Contractual Clauses, together with any additional measures needed.

9.2. Travel Rule information may need to be sent to a counterparty CASP outside the EEA when you transfer crypto-assets to it. In that case we assess the counterparty's ability to protect the data, as required by Regulation (EU) 2023/1113 and applicable guidance.

9.3. You can obtain more information about the safeguards we use by contacting the DPO.

10. RECORDING OF COMMUNICATIONS

10.1. We record and keep telephone conversations and electronic communications with you that relate to our services, including chats and emails, as required by MiCA. We use these records to evidence your instructions, resolve disputes, monitor service quality, train staff and meet regulatory requirements. A copy is available to you on request.

11. HOW LONG WE KEEP PERSONAL DATA

11.1. We keep personal data only for as long as necessary for the purposes for which it was collected. In particular:

- customer due diligence documents, transaction records and Travel Rule information are kept for at least five (5) years after the end of our business relationship, as required by Law 188(I)/2007 and Regulation (EU) 2023/1113;
- records of our services, orders, transactions, communications and agreements with you are kept for five (5) years and, where CySEC requests it before that period ends, for up to seven (7) years, as required by MiCA;
- where you have opted out of marketing, we keep your contact details on a suppression list so that we do not contact you again; and
- we may keep personal data for longer where needed in connection with an investigation, legal claim or request from a competent authority.



11.2. When personal data is no longer needed, we securely delete it or anonymise it.

12. YOUR RIGHTS

12.1. Subject to the conditions and exceptions in the GDPR, you have the right to:

- **access** your personal data and receive a copy of it;
- **rectify** inaccurate or incomplete personal data;
- **erase** your personal data, except where we must keep it to comply with the law or to establish, exercise or defend legal claims;
- **restrict** our processing of your personal data in certain circumstances;
- **object** to processing based on our legitimate interests, and to object at any time to direct marketing;
- **data portability**, meaning to receive personal data you provided to us in a structured, commonly used and machine-readable format, or to have it sent to another controller, where processing is based on consent or contract and carried out by automated means;
- **withdraw consent** at any time, without affecting the lawfulness of processing before withdrawal; and
- **not be subject to a decision based solely on automated processing** that produces legal or similarly significant effects, and to request human intervention (see section 7).

12.2. To exercise any of these rights, email dpo@nagax.com. We may need to verify your identity before responding. We will respond within one (1) month of receiving your request. This period may be extended by up to two (2) further months for complex or numerous requests, in which case we will tell you why. Exercising your rights is free of charge, unless a request is manifestly unfounded or excessive.

12.3. Some of your rights are limited by our legal obligations. For example, we cannot delete records we are required to keep under MiCA or anti-money laundering law before the retention period ends, and we may be prohibited by law from disclosing certain information, such as a report made to MOKAS.

13. SECURITY OF PERSONAL DATA

13.1. We use appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. These include encryption, multi-factor authentication, role-based access controls limited to staff who need the data for their duties, logging and monitoring, secure development practices, staff training and regular testing of our controls.

13.2. We carry out data protection impact assessments before starting processing that is likely to result in a high risk to individuals, such as the introduction of new technologies.

13.3. Please keep your log-in details confidential. We will never ask you for your password or two-factor authentication codes.

14. PERSONAL DATA BREACHES

14.1. We maintain procedures to detect, assess and respond to personal data breaches. Where required by the GDPR, we will notify the Commissioner for Personal Data Protection within 72 hours of becoming aware of a breach. If a breach is likely to result in a high risk to your rights and freedoms, we will inform you without undue delay.

15. SOCIAL NETWORKS

15.1. We maintain pages on social networks, including those operated by Meta (Facebook and Instagram), Google (YouTube), X, TikTok and LinkedIn, to communicate with you and provide information about our



services. When you interact with these pages, the network operator processes your personal data under its own privacy policy, and may provide us with aggregated statistics about the use of our pages.

15.2. For some networks, including Facebook and LinkedIn, we act as joint controllers with the operator for the statistics we receive, under agreements published by those operators. To exercise your rights in relation to data processed by a social network, it is usually most effective to contact the network directly.

15.3. We do not use publicly available social network information for purposes other than customer due diligence, fraud prevention and our legal obligations.

16. COOKIES

16.1. We use cookies and similar technologies on the Website and Platform. Non-essential cookies are used only with your consent. Details are set out in our Cookies Policy, available at <https://nagax.com/eu>.

17. CHANGES TO THIS POLICY

17.1. We may update this Policy to reflect changes in law, regulatory guidance or our services. The current version is always available on the Website. Where we make a material change, we will notify you by email or through the Platform before it takes effect.

18. COMPLAINTS

18.1. If you have a concern about how we use your personal data, please contact our DPO first at dpo@nagax.com, and we will try to resolve it.

18.2. You also have the right to lodge a complaint with the Commissioner for Personal Data Protection of the Republic of Cyprus (P.O. Box 23378, 1682 Nicosia, Cyprus; commissioner@dataprotection.gov.cy; www.dataprotection.gov.cy), or with the data protection supervisory authority in the EU/EEA Member State where you live or work, or where the alleged infringement took place.