



NAGA

Privacy Policy

Updated Version: January 2025

Contents

1.	ABOUT US.....	3
2.	OUR COMMITMENT.....	3
3.	PURPOSE OF THIS POLICY	3
4.	AMENDMENTS	4
5.	WHAT PERSONAL DATA WE COLLECT AND HOW	4
6.	DISCLOSURE OF YOUR PERSONAL DATA.....	10
7.	INTERNATIONAL TRANSFERS OF YOUR PERSONAL DATA.....	12
8.	HOW WE USE YOUR PERSONAL DATA AND LEGAL BASES FOR PROCESSING	12
9.	ONLINE PRESENCE IN SOCIAL NETWORKS.....	17
10.	TECHNICAL AND OPERATIONAL SECURITY MEASURES	19
11.	AUTOMATED DECISION-MAKING AND PROFILING.....	19
12.	COMMUNICATION	20
13.	STORAGE AND RETENTION OF YOUR PERSONAL DATA	20
14.	WHAT ARE YOUR RIGHTS AS A DATA SUBJECT?	21
15.	PERSONAL DATA BREACH	23
16.	COMPLAINTS WITH REGARDS TO THE USE OF PERSONAL DATA	23

1. ABOUT US

NAGA X LTD (hereafter referred to as “**NAGA**”, and/or the “**Company**” and/or “**we**” and/or “**us**”) is a Cypriot Crypto Asset Services Provider (“**CASP**”) registered with the Registrar of Companies in Cyprus under number HE 424746 and regulated by the Cyprus Securities and Exchange Commission (“**CySEC**”) under registration number 009/23. NAGA is part of the wider NAGA Group of Companies of The NAGA Group AG and all its direct or indirect subsidiaries and/or direct or indirect parent undertakings, including but not limited to: NAGA GLOBAL LLC, NAGA Markets Europe Ltd, NAGA Technology GmbH, and NAGA Pay GmbH, as well as any subsidiary and/or any holding company from time to time of any of the aforementioned companies, and any subsidiary from time to time of a holding company of that company (hereafter referred to as “**NAGA Group**”). NAGA is the ‘controller’ of your personal data – this means that NAGA determines the purposes and means of the processing of your personal data as expressly provided in this Privacy Policy (hereafter referred to as the “**Policy**”).

2. OUR COMMITMENT

Your privacy is of utmost importance to us, and it is our priority to safeguard and respect the confidentiality of your information, your privacy, and your rights. By entrusting us with your information, we would like to assure you of our commitment to keep such information private and secure. We have taken all the required technical and organisational steps to protect the confidentiality, security and integrity of your personal information and adhere to applicable statutory data protection requirements, including but not limited to the General Data Protection Regulation (“**GDPR**”), as illustrated herein.

3. PURPOSE OF THIS POLICY

This Policy sets out how and what personal data NAGA processes while using NAGA’s official website at www.nagax.com (hereafter referred to as the “**Website**”), the NAGA App (hereafter referred to as the “**App**”) and social networks whereby we maintain online presences (hereafter referred to as the “**Social Networks**”), including any personal data you may provide through this Website, App and Social Networks when you obtain our services. For the purposes of this Policy:

- ‘**personal data**’ or ‘**data**’ means any information relating to an identified or identifiable natural person (‘data subject’, ‘you’, ‘your’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- ‘**processing**’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

It also provides information on how and what personal data we may collect from third parties. Additionally, it provides information on how you can exercise your rights with respect to the processing of your personal data. This Policy applies to the processing activities performed by NAGA to the personal data of its clients and potential clients, website and app visitors and users as in order to provide our products and services to you we need to collect your personal information as specified in this Policy.

Our services are not aimed at children under 18 years. We do not knowingly collect information from children under the age of 18. If you have not reached the age limit, do not use the services and do not provide us with your personal information. If you are a parent of a child below the age limit and you learn that your child has provided us with personal information, please contact us on the following information, in order to exercise your rights as explained in more detail below.

Additionally, if you have concerns about how we use your personal data, or requests on how to exercise your legal rights, please use the contact details below:

Entity: NAGA X Ltd

Contact Person: Data Protection Officer

Email address: dpo@nagax.com

Postal address: Agias Zonis, 11, 3027 Limassol, Cyprus

4. AMENDMENTS

The Company reserves the right to amend this document from time to time and we will notify you appropriately and accordingly. We do however encourage you to review this statement periodically to be always informed about how we are processing and protecting your personal data and contact us at dpo@nagax.com if you have any concerns.

5. WHAT PERSONAL DATA WE COLLECT AND HOW

The table below includes the type of personal data we process and how we collect it:

Type of personal data	Details
Information you provide to us	We collect information you provide when you: <ul style="list-style-type: none">▪ fill in any forms▪ correspond with us▪ respond to any of our surveys▪ register to use the NAGA App▪ open an account or use any of our services pursuant to the terms and conditions of the Client Agreement

	<ul style="list-style-type: none">▪ transacting in cryptocurrencies▪ take part in online discussions or promotions▪ speak with a member of our Social Networks or customer support teams (either on the phone or through the NAGA app)▪ access, browse and/or use the NAGA feed▪ share information with us on Social Networks▪ contact us for other reasons <p>We will collect the following information:</p> <ul style="list-style-type: none">▪ your full name, surnames as per your National ID, title, date and place of birth, nationality, citizenship, country of residence, national ID number, marital status▪ your phone number, email address, residential address, and proof of address (such as a utility bill or bank statement)▪ investment education experience, risk appetite, capacity for loss, tax status▪ employment status, occupation (work industry), net annual income, main source of income, net worth, source of funds, anticipated account turnover and other financial information▪ if you are a legal person, we will collect the name under which you are registered and/or the trading name of the company▪ if you are a legal person, we will collect your LEI or equivalent number▪ details of the device you use (for example, your phone, computer or tablet) <p>your NAGA username, account number and ID (these are random and are</p>
--	--

	<p>automatically assigned to you when you join), your password, preferences, feedback and survey responses and marketing and communication data such as your preferences in receiving marketing from us and our third parties and your communication preferences</p> <ul style="list-style-type: none">▪ your registration information▪ details of your bank account, including the account number, sort code and IBAN▪ details of your debit cards and credit cards (or other debit or credit cards you have registered with us) - only the four last digits of your card number, expiry date and name printed on the card▪ copies of your identification documents (for example, your ID, passport or driving license) and any other information you provide to prove you are eligible to use our services▪ your country of residence, tax residency information, and tax identification number▪ records of our discussions, written or oral, if you contact us or we contact you (including records of phone calls)▪ your image in photo or video form (where required as part of our Know-Your-Customer (KYC) checks, to verify your identity, or where you upload a photo to your NAGA account)
--	--

<p>Information collected from your use of our products, services and website/app by using cookies (as per our Cookie Policy), and other similar technologies.</p>	<p>Whenever you use our website or the NAGA app and/or any other platforms in relation to NAGA's services, we collect the following information:</p> <ul style="list-style-type: none">▪ technical information, including the internet protocol (IP) address used to connect your computer to the internet, country (by IP), your login information, the browser type and version, the time zone setting, the operating system and platform, the type of device you use, a unique device identifier (for example, your device's IMEI number, the MAC address of the device's wireless network interface, or the mobile phone number used by the device), mobile network information, your mobile operating system and the type of mobile browser you use▪ information about your visit, including the links you've clicked on, through and from our website or app (including date and time), services you viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling and clicks), and methods used to browse away from the page▪ information on transactions and your use of NAGA products (for example, your exchange activity), details of deposits, deposit methods, details of withdrawal, withdrawal methods, details of your exchange activity through NAGA, including the date, time, amount, cryptocurrencies, exchange rate, details of device used
---	---

	to arrange the payment and the payment method used
Information collected from your use of our Social Networks and/or NAGA's social feed.	<p>We collect statistics on the use of our online presences, which are provided by the Social Networks.</p> <p>These statistics are aggregated and may include, in particular, demographic information and data on interaction with our online presences and the posts and content distributed through them.</p> <p>Your data is usually processed by the Social Networks concerned for market research and advertising purposes. In this way, usage profiles can be created based on the interests of the users. For this purpose, cookies and other identifiers are stored on your computers. On the basis of these usage profiles, advertisements, for example, are then placed within the Social Networks but also on third-party websites.</p> <p>For more details you may refer to Section 9 below, since in many cases we do not control the data collected from the use of Social Networks and you may opt-out via the Social Networks' privacy policy and/or privacy options.</p>
Information about your location	We track your location via your IP address
Information from others	<p>We collect personal data from third parties or other people, such as financial or credit institutions, CASPs, official and/or other registers and databases, fraud prevention agencies and partners who help us to provide our services, as well as other Affiliates.</p> <p>This includes information to help us check your identity, information about your spouse and family and/or associate (if applicable in the context of a potential Third Party Payment), information of your IP address information when you are referred to us to register an account.</p>

	<p>We collect information on the beneficiary VASP/CASP such as full name and account number or unique reference number. This information will help us identify the beneficiary of the transaction.</p> <p>Technical data from analytics providers such as Google based outside of EU.</p> <p>In some cases, third parties, such as Affiliate partners you interact with, may share information about you with us, whereby they act as individual ‘controllers’. In such circumstances we ensure that the relevant provisions of GDPR are respected and any information we receive about you has been provided with your prior consent. Even though we make sure that we enter into data sharing agreements in order to safeguard your data, we would also advise you to consult their Privacy Policy prior to registering a NAGA account with us or providing any information to us since we are not responsible for any information you disclose to such third parties before entering our Website or App.</p>
Information from Social Networks	Occasionally, we’ll use publicly available information about you from selected Social Network websites or apps to carry out enhanced due diligence checks. Publicly available information from Social Network websites or apps may also be provided to us when we conduct general searches on you (for example, to comply with our anti-money laundering or sanctions screening obligations).
Information from publicly available sources	We collect information and contact details from publicly available sources, such as media stories, online registers or directories, and websites for enhanced due diligence checks, security searches, and KYC purposes.

6. DISCLOSURE OF YOUR PERSONAL DATA

The Company may share your personal data for the purposes of processing transactions and providing services relating to your account, as well as to secure our legitimate interests and legal obligations regarding suspected abuse of anti-money laundering rules with any NAGA Group entity or beneficiary VASPs/CASPs. Such sharing of data in NAGA Group includes and is not limited to the data and documents collected by the Company for identification purposes. Sharing personal data with beneficiary VASPs/CASPs includes but is not limited to full names and surnames, account number and physical address.

The Company may also share your personal data with service providers in the areas of IT, translation of documents, marketing, auditors, background screening providers, financial institutions, funds, payment recipients, payment and settlement infrastructure providers, exchanges, regulators, public authorities (including tax authorities), our other group entities and service providers, professional advisers, insurers and potential purchasers of elements of our business.

Where it is required to disclose your personal data to third parties for the purposes of performing our legal obligations towards you, we ensure that the relevant provisions of GDPR are respected. Specifically, we assess these third parties in respect of their compliance with the data protection laws and regulations and ensure that required contractual agreements are concluded. Respectively, we ensure that they are committed to respecting the security of your information and treat it in accordance with relevant laws and regulations. Finally, we do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions, where such third parties act as our 'processors'.

In some cases, we may disclose your personal data to third parties, such as Payment Service Providers you may use to fund your account, whereby they act as individual 'controllers'. Even though we make sure that we enter into data sharing agreements, in order to safeguard your data, we would also advise you to consult their Privacy Policy prior to using their services, since we are not responsible for any further information you may disclose to such third parties and/or how they process your data if you choose to make use of their services, since any such information that we share with such a third-party will be used and disclosed in accordance with the third-party's privacy practices.

The table below explains which suppliers we normally share your personal data with:

Type of supplier	Why we share your personal data
Suppliers who provide us with IT and payment services	To help us provide our services to you
Beneficiary VASPs/CASPs	To facilitate the transactions

EMI, Bank Institutions, Payment Institutions	To safekeep your assets and/or execute your deposits/withdrawals
Administrative systems (KYC onboarding service providers, translation, due diligence, finance, reporting, risk analysis)	To help us perform checks in order to decide whether to provide our services to you and to maintain our daily operations
Internal Auditors	To help us comply with our legal obligations
Analytics providers and search information providers	To help us improve our website or app
Customer-service providers, survey providers and developers	To help us to provide our services to you
Communications services providers	To help us send you emails, push notifications and text messages
Data storage	To store your data

We may also share your personal data with government authorities, law enforcement authorities, tax authorities, companies and fraud prevention agencies to check your identity, protect against fraud, keep to tax laws, anti-money laundering laws, or any other laws and confirm that you're eligible to use our products and services. If fraud is detected, you could be refused certain services by NAGA or other NAGA Group entities.

We may also need to share your personal data with other third-party organisations or authorities, for legal reasons, such as:

- if we have to do so under any law or regulation
- if we sell our business
- in connection with criminal or fraud investigations
- to enforce our rights (and those of clients or others)
- in connection with legal claims.

Where you direct us to share your personal data with a third party, we may do so. For example, you may authorise third parties to act on your behalf (such as a lawyer, accountant or family member or guardian under a power of attorney). We may need to ask for written proof that a third party has been validly authorised to act on your behalf.

7. INTERNATIONAL TRANSFERS OF YOUR PERSONAL DATA

Sometimes we may need to transfer your personal data outside the European Economic Area (EEA) to help us provide our services to you. For example, we may disclose your personal data to keep to global legal and regulatory requirements, to provide ongoing support services, to credit reference agencies, fraud prevention agencies, law enforcement authorities and to enable us to provide you with products or services you have requested. Please be informed that, whenever we transfer your personal data out of the EEA, we ensure that a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- we will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission;
- we will make sure that a contract with strict data protection safeguards is in place before we transfer your personal data, such as a Data Sharing Agreement and
- where we use certain service providers, we use specific contracts approved by the European Commission which give personal data the same protection it has in Europe, such as Standard Contractual Clauses.

Should you need further clarifications on this, please contact us at dpo@nagax.com.

8. HOW WE USE YOUR PERSONAL DATA AND LEGAL BASES FOR PROCESSING

The Company may process your personal data in various ways and for that rely on specific legal bases. Please be informed however, that we may process your personal data for more than one lawful basis and depending on the specific purpose for which we will use them. The purposes for which we may process your personal data are explained below in more detail.

THE FRAMEWORK OF THE CLIENT AGREEMENT (PERFORMANCE OF CONTRACT): We process personal data to provide our services and products, as well as information regarding these services and products, based on our contractual relationship with you. We need, therefore, to use your personal data in order to perform our services and comply with our contractual obligations to you. In this framework, we need to verify your identity to accept you as our client, and we will need to use those personal details to effectively manage your account with us.

COMPLIANCE WITH LAWS AND REGULATIONS (LEGAL OBLIGATION): numerous laws to which we are subject to, as well as specific statutory requirements (such as anti-money laundering laws, Cyprus Securities and Exchange Commission (CySEC) laws and regulations, financial services laws, corporation laws, privacy laws and taxation laws) dictate that we hold and process personal data. Such obligations and requirements impose on us necessary personal data storage and processing activities. It is mandatory, for example, to store personal data, for record-keeping purposes. In general, complying with applicable laws, court orders, other judicial process, or the requirements of any applicable regulatory authorities may require the processing of personal data by NAGA.

SAFEGUARDING OUR INTERESTS (LEGITIMATE INTERESTS): We process personal data to safeguard the legitimate interests pursued by NAGA. Examples of such processing activities include our initiating legal claims and preparing our defense in litigation procedures and processing personal data for risk management purposes. Further, we may need to use personal information collected from you to investigate issues or to settle disputes with you because it is in our legitimate interests to ensure that issues and disputes get investigated and resolved in a timely and efficient manner. We may also implement procedures based on specific and limited criteria to exchange data regarding suspected abuse of anti-money laundering rules with NAGA Group, with strict limitation on access, security and prohibition of any further use for other purposes.

CASES YOU HAVE CONSENTED TO: We may process your personal data in order to provide direct marketing about our products or services, whereby your explicit consent is required. Please be informed that, if we rely on your consent as our legal basis for holding and processing your personal information, **you have the right to revoke consent at any time, by contacting us at dpo@nagax.com.** However, any processing of personal data that took place prior to the receipt of your revocation will not be affected. If you have consented to be contacted by us for marketing purposes, we may use your personal information to send you marketing communications by email or phone or other agreed forms to ensure that you are kept up to date with our latest products and services. We will not disclose your information to any third parties for them to directly market to you.

What we use your personal data for	Our legal basis for using your personal data
<p>Providing our services</p> <p>Whenever you sign up with NAGA, apply for or use a product or service, we'll use your personal data to:</p> <ul style="list-style-type: none"> ▪ check your identity (as part of our KYC process) ▪ decide whether or not to approve your application ▪ meet our contractual and legal obligations relating to any products or services you use (for example, any exchange activity from your NAGA account, withdrawing or depositing any amount in your NAGA account with your credit/debit card or otherwise) ▪ facilitate crypto transactions ▪ maintain your personal profile 	<ul style="list-style-type: none"> ▪ Keeping to contracts and agreements between you and us ▪ Legitimate interests (we need to be efficient about how we meet our obligations and we want to provide you with good products and services) ▪ Legal obligations ▪ Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Text with EEA relevance)

<ul style="list-style-type: none"> ▪ monitor your exchange activity and transactions in order to ensure and/or monitor execution quality. ▪ we may need to inform you of changes to the terms or the features of our products or services. ▪ provide you with customer support services. We record and monitor all our communications between you and us, including phone calls, to maintain appropriate records, check your instructions, analyse, assess and improve our services, and for training and quality control purposes 	
<p>Protecting against fraud</p> <p>We use your personal data to check your identity to protect against fraud, keep to financial crime laws and to confirm that you're eligible to use our services. We also use it to help us better understand your financial circumstances and manage fraud risks related to your NAGA account.</p>	<ul style="list-style-type: none"> ▪ Legitimate interests (to develop and improve how we deal with financial crime and meet our legal responsibilities) ▪ Legal obligations
<p>Marketing and providing products and services that might interest you</p> <p>We use your personal data to do the following:</p> <ul style="list-style-type: none"> ▪ to personalise your in-app experience and marketing messages about our products and services so they are more relevant and interesting to you (where allowed by law). This may include analysing how you use our products, services and your transactions ▪ if you agree, provide you with information about our partners' promotions or offers which we think you might be interested in ▪ if you agree, allow our partners and other organisations to provide you with information about their products or services 	<ul style="list-style-type: none"> ▪ Legitimate interests (to send direct marketing, ensure our direct marketing is relevant to your interests, develop our products and services, and to be efficient about how we meet our legal and contractual duties) ▪ Consent (where we're legally required to get your consent to send you direct marketing about our products or services, or partners' promotions or offers, or for you to receive marketing from other organisations)

<ul style="list-style-type: none"> ▪ measure or understand the effectiveness of our marketing and advertising, and provide relevant advertising to you ▪ ask your opinion about our products or services <p>Remember, you can ask us to stop sending you marketing information by opting out of your marketing choices</p>	
<p>To keep our services up and running</p> <p>We use your personal data to manage our website and the NAGA app, (including troubleshooting, data analysis, testing, research, statistical and survey purposes), and to make sure that content is presented in the most effective way for you and your device.</p> <p>We also use your personal data to:</p> <ul style="list-style-type: none"> ▪ verify your identity if you contact our customer support or social media teams ▪ allow you to take part in interactive features of our services ▪ tell you about changes to our services ▪ help keep our website and the NAGA app safe and secure 	<ul style="list-style-type: none"> ▪ Keeping to contracts and agreements between you and us ▪ Legitimate interests (to be efficient about how we meet our obligations and keep to regulations that apply to us and to present content as effectively as possible for you) ▪ Consent (where required by law)
<p>Location-based monitoring</p> <p>While using your NAGA account via website or app, we use your personal data to:</p> <ul style="list-style-type: none"> ▪ protect against fraud 	<ul style="list-style-type: none"> ▪ Keeping to contracts and agreements between you and us ▪ Legitimate interests (to develop and market our products and keep to regulations that apply to us)
<p>Preparing anonymous statistical datasets</p> <p>We prepare anonymous statistical datasets about our clients' exchange activity patterns:</p> <ul style="list-style-type: none"> ▪ for forecasting purposes 	<ul style="list-style-type: none"> ▪ Legitimate interests (to conduct research and analysis, including to produce statistical research and reports) ▪ Legal obligations

<ul style="list-style-type: none"> ▪ to understand how clients use NAGA products and services ▪ to comply with governmental requirements and requests <p>These datasets may be shared internally in NAGA Group or externally with others, including non-NAGA Group companies. We produce these reports using information about you and other Clients. The information used and shared in this way is never personal data and you will never be identifiable from it. Anonymous statistical data cannot be linked back to you as an individual.</p> <p>For example, some countries have laws that require us to report spending statistics and how money enters or leaves each country. We'll provide anonymised statistical information that explains the broad categories of merchants that NAGA clients in that country spend their money with. We'll also provide information about how NAGA clients top up their accounts and transfer money. However, we won't provide any client-level information. It will not be possible to identify any individual NAGA client.</p>	
<p>Improving our products and services</p> <p>We may send you surveys as part of our customer feedback process. It is in our legitimate interest to ask for such feedback to try to ensure that we provide our services and products at the highest standards. We may use the personal information provided by you through such client surveys to help us improve our products and services.</p>	<ul style="list-style-type: none"> ▪ Legitimate interests (to understand how clients use our products so we can develop new products and improve the products we currently provide)
<p>Meeting our legal obligations, enforcing our rights and other legal uses</p> <p>We use your personal data:</p> <ul style="list-style-type: none"> ▪ to share it with other organisations (for example, government authorities, law enforcement authorities, VASPs/CASPs, tax authorities, fraud 	<ul style="list-style-type: none"> ▪ Legitimate interests (for example, to protect NAGA during a legal dispute) ▪ Substantial public interest (if we process your sensitive personal data to keep to

<p>prevention agencies, our regulator CySec or any other regulatory authority having control or jurisdiction over us or you or our associates or in whose territory we have clients or service providers and as applicable)</p> <ul style="list-style-type: none"> ▪ To share it with VASPs/CASPs to combat money laundering and terrorism financing ▪ occasionally advise you of certain changes to products or services or laws (as we are required to do so by laws and regulations). ▪ to manage the risk and optimise the efficiency of our group operations ▪ if this is necessary to meet our legal or regulatory obligations ▪ in connection with legal claims ▪ to help detect or prevent crime 	<p>legal requirements that apply to us)</p> <ul style="list-style-type: none"> ▪ Legal obligations ▪ Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Text with EEA relevance)
--	---

9. ONLINE PRESENCE IN SOCIAL NETWORKS

We maintain online presences in Social Networks in order to communicate there with you and interested individuals, among others, and to provide information about our products and services.

As part of the operation of our online presence, it is possible that we can access information such as statistics on the use of our online presence, which are provided by the Social Networks, as explained in the table above (in Section 5). You may refer to the list below for details to the data of the Social Networks that we can access as operators of the online presences.

The legal basis for data processing is the performance of a contract with you and consent (where applicable), in order to stay in contact with you and to carry out pre-contractual measures with future clients and interested parties.

For the legal basis of the data processing carried out by the Social Networks on their own responsibility, please refer to the data protection information of the respective Social Network. In many circumstances you have option to object to the processing of your data, in which case you may refer to the privacy policy options of each Social Network.

We would like to point out that data protection requests can be asserted most efficiently with the respective provider of the Social Network, as only these providers have access to the data and can take appropriate measures directly. Below is a list with information on the Social Networks on which we operate online presences:

- **Facebook** (USA and Canada: Facebook Inc., 1601 Willow Road, Menlo Park, California 94025, USA; all other countries: Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland).
 - The operation of the Facebook Fanpage is in joint responsibility on the basis of an agreement on joint processing of personal data, which can be found on Facebook. That means that we act as joint controllers with the Social Network.
- **Instagram** (Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland).
- **Google / YouTube** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland).
- **Twitter** (Twitter International Company, One Cumberland Place, Fenian Street, Dublin 2, D02 AX07 Ireland).
- **TikTok** (TikTok Technology Limited, 10 Earlsfort Terrace, Dublin, D02 T380, Ireland).
- **LinkedIn** (LinkedIn Ireland Unlimited Company Wilton Place, Dublin 2, Ireland).
 - The operation of the LinkedIn page is in joint responsibility on the basis of an agreement on joint processing of personal data which can be found on LinkedIn. That means that we act as joint controllers with the Social Network.
- **Google my business**
 - We operate a so-called Google My Business entry. Should you find us in this way, we make use of the information service offered by Google and the services of Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland (hereafter “Google”).
 - We would like to point out that you use the Google site and its functions on your own responsibility. This applies in particular to the use of the social and interactive functions (e.g. commenting, sharing, rating, direct messaging). When you visit and interact with our Google My Business listing, Google also collects your IP address and other information that is present on your terminal device in the form of so-called cookies. This information is used to provide us, as the operator of the Google My Business listing, with statistical information about the use of Google services. The data collected about you in this context will be processed by Google and may be transferred to countries outside the European Union. You may find more information about how Google processes personal data in Google’s privacy policy.
 - We do not know how Google uses the data from the visit for its own purposes, to what extent activities of individual users are assigned, how long Google stores this data and whether data is passed on to third parties. When accessing Google services, the IP address assigned to your terminal device is transmitted to Google. Google also stores information about its users’ end devices; this may enable Google to assign IP addresses to individual users or user accounts.
 - If you contact us via our Google My Business entry or other Google services by direct message, we cannot rule out the possibility that these messages may also be read and evaluated by Google (both by employees and automatically). We therefore advise against providing us with personal data there. Instead, another form of communication should be chosen as early as possible. The use of this service is subject to the Google Privacy Policy, which you – with use – have already agreed to.

- We, as the provider of our Google My Business entry, do not collect or process any further data from your use of this Google service.

10. TECHNICAL AND OPERATIONAL SECURITY MEASURES

The Company has adopted practice controls and security measures to ensure high level of information security and compliance with the relevant provisions of GDPR. Indeed, our administrative, physical, and technical safeguards that are implemented and maintained, protect your personal data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, sorted, or otherwise processed. Employees are authorized to access personal data only to the extent necessary to serve the applicable legitimate purposes for which the personal data are processed by the Company and to perform their duties.

The Company shall also conduct a Data Protection Impact Assessment (DPIA) in relation to any operation that may be likely to result in a high risk to the rights and freedoms of any data subject, in particular, in the use of new technologies. This DPIA shall be conducted prior to any processing takes place, regarding all activities, projects and systems involving the processing of personal data and taking into account the nature, scope, context and purposes of such processing.

Please be mindful not to share or disclose your log in details with any third party.

Details of these measures may be available upon request at dpo@nagax.com and to our discretion.

11. AUTOMATED DECISION-MAKING AND PROFILING

The Company is required to assess your knowledge and experience, your financial situation and investment objectives and your risk profile once per calendar year in accordance with relevant laws and regulations. This action is in accordance with Anti-money laundering (AML) Law and CySec Laws, Regulations and related Circulars and guidelines on this matter. The tools used on the above include the Appropriate Test as follows:

- The **Appropriateness Test** occurs once you register as a client at NAGA where we need to check and ensure that you are suitable for the provision of services and products we offer. This test is regarding your knowledge, financial background and experience with financial services and based on the scoring you receive, you will be informed whether you are eligible to receive our services and become our client and the maximum level of leverage you are eligible to. This ensures that our services and products are suitable to you and to the best of our interests.

This means that we sometimes use technology that can evaluate your personal circumstances and other factors to predict risks or outcomes. We do this for the efficient running of our services and to ensure decisions are fair, consistent and based on the right information. We further use this technology:

- When opening client accounts for the performance of KYC, anti-money laundering, sanctions checks, identity and address checks; and
- For detecting fraud by monitoring your account to detect fraud and financial crime.

Where we make an automated decision about you, you have the right to ask that it is manually reviewed by a person as explained in your Rights (in Section 14) below.

We assure you that NAGA takes all the technical and operational measures to correct inaccuracies and minimize the risk of errors, to prevent any discrimination and to secure your personal data.

The scorings above are monitored by the Compliance department of NAGA and should you need any clarification, you may contact us at dpo@nagax.com.

12. COMMUNICATION

The Company will record, monitor and process any telephone conversations and/or electronic communications you have with us such as via phone, email, Social Networks or electronic message. All such communications are recorded and/or monitored and/or processed by us, including but not limited to any telephone conversations and/or electronic communications that result or may result in transactions or client order services even if those conversations or communications do not result in the conclusion of such transactions. All incoming and outgoing telephone conversations as well as other electronic communications between you and NAGA will be recorded and stored for quality monitoring, training and regulatory purposes. The content of relevant in person conversations and/or communications with you may be recorded by minutes or notes. Any such records shall be provided to you upon request at the same language as the one used to provide our services to you.

13. STORAGE AND RETENTION OF YOUR PERSONAL DATA

NAGA retains your personal information on secure servers and appropriate procedures and measures are in place to ensure that your personal data is safeguarded as this is of utmost importance to us. We will hold your personal information while we have a business relationship with you and as permitted by relevant laws and regulations. The retention of your personal data is limited for the purposes we collected it for and in order for us to comply with any legal, regulatory, accounting, taxation or reporting requirement. To determine the appropriate retention period for personal data, in accordance with the provisions of GDPR, we consider various factors including, but not limited to, the amount, nature, and sensitivity of the personal data, and the potential risk of harm from unauthorised use or disclosure of your personal data.

Moreover, when we consider that personal information is no longer necessary for the purpose for which it was collected, we will remove any details that will identify you or we will securely destroy the records. However, we may need to maintain records for a significant period of time. For example, we are subject to certain anti-money laundering and taxation laws which require us to retain the

following, for a period of seven (7) years after our business relationship with you has ended:

- a copy of the documents we used in order to comply with our customer due diligence obligations;
- supporting evidence and records of transactions with you and your relationship with us;
- communication records between us.

Also, the personal information we hold in the form of a recorded communication, by telephone, electronically, in person or otherwise, will be held in line with local regulatory requirements (i.e., 7 years after our business relationship with you has ended or longer in order to secure our legitimate interests (such as handling a dispute with you). If you have opted out of receiving marketing communications we will hold your details on our suppression list so that we know you do not want to receive these communications.

We may keep your personal data for longer because of a potential or ongoing court claim, or for another legal reason.

14. WHAT ARE YOUR RIGHTS AS A DATA SUBJECT?

You must be aware that GDPR is recognising you as a “**Data subject**” and you have certain rights which you can exercise freely and to your own discretion, as per below:

- **Request access to your personal information:** this enables you to be informed of what data we process about you, how we process the data, to receive a copy of it and to check that we are lawfully processing it. We cannot give you any personal data about other people, personal data which is linked to an ongoing criminal or fraud investigation, or personal data which is linked to settlement negotiations with you. We also will not provide you with any communication we have had with our legal advisers
- **Request correction of the personal information that we hold about you:** this enables you to have any incomplete or inaccurate information we hold about you corrected. Before we update your file, we may need to check the accuracy of the new personal data you have provided.
- **Request erasure of your personal data:** this enables you to ask us to delete or remove personal data where: (i) there is no good reason for us to continue using it; (ii) you gave us consent (permission) to use your personal data and you have now withdrawn that consent; (iii) you have objected to us using your personal data; (iv) we have used your personal data unlawfully; (v) the law requires us to delete your personal data. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request. If you have terminated your agreement with us or closed your NAGA account, we may not be able to delete your entire file because our regulatory responsibilities take priority. We will always let you know if we cannot delete your personal data.

- **Object to processing of your personal data where we are relying on a legitimate interest** (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. However, if there is an overriding reason why we need to use your personal data, we will not accept your request. If you object to us using personal data which we need in order to provide our services, we may need to close your account as we will not be able to provide the services.
- **Request the restriction of processing of your personal data:** this enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- **Request the transfer of your personal data to you or to a third party:** we will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format - if we can, and are allowed to do so under regulatory requirements. Note that this right only applies when (i) the lawful basis for processing your information is consent or for the performance of a contract; and (ii) the processing of your data was carried out by automated means (i.e. excluding paper files) and it does not include any additional data that we may have created based on the data that you have provided to us (for example, if we use the data you have provided to create a user profile for you, then this data would not be in the scope of this right).
- **Right to withdraw consent:** where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.
- **Human review of an automated decision:** where we make an automated decision about you that significantly affects you, you can ask us to carry out a manual review of this decision.

If you wish to exercise any of the above, you must send an email at dpo@nagax.com and your request will be further handled. Your ability to exercise these rights will depend on a number of factors. Sometimes, we will not be able to agree to your request (for example, if we have a legitimate reason or a legal obligation for not doing so or the right does not apply to the particular information we hold about you)

Please be informed of the following:

- a. usually no fee is required in order to exercise your rights, but we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive; or refuse to comply with your request in these circumstances

- b. we reserve the right to request specific information to confirm your identity, speed up our response and ensure your right to access your personal data or any other right as data subject
- c. we will always respond to your request within reasonable time and keep you updated.

15. PERSONAL DATA BREACH

We have put in place appropriate procedures in order to deal with any breach of personal data and will notify you and any applicable regulator of a breach where we are legally required to do so.

16. COMPLAINTS WITH REGARDS TO THE USE OF PERSONAL DATA

Should you wish to report a complaint or if you feel that we have not addressed your concern in a satisfactory manner, you may contact the Personal Data Protection Commissioner's Office.

Website: <http://www.dataprotection.gov.cy/>

Email: commissioner@dataprotection.gov.cy

Address: Iasonos 1, 1082 Nicosia, Cyprus