PRIVACY POLICY

Version 1 – April 2024

TABLE OF CONTENTS

1. ABOUT US

This is the Privacy Policy (hereafter referred to as the "**Policy**") of Axon Securities S.A. (hereinafter referred to as "**Axon**" and/or the "**Company**" and/or "**we**"), a company incorporated in Greece with registration number 000708201000, authorized and regulated by the Hellenic Capital Market Commission (hereafter referred to as "**HCMC**") as a Greek Investment Firm with license number 32/315/26.10.2004 to offer certain investment and ancillary services subject to the provisions of the Law 4514/2018 "Markets in financial instruments and other provisions".

The Company's registered address is at 48 Stadiou Street, 105 64 Athens, Greece.

NAGA.eu is the Company's domain/website, which is owned by Naga Technology GmbH, however, is independently and exclusively operated by Axon Securities S.A.

NAGA is a trade name and trademark under the NAGA Group AG, a German based FinTech company publicly listed on the Frankfurt Stock Exchange. Exclusive rights for the use of the said trade name and trademark, in the territory of Greece, are exclusively granted to Axon Securities S.A.

2. OUR COMMITTEMENT

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 respect your personal data and act in accordance with the privacy and data protection legislation. 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 (hereinafter referred to as "**GDPR**"), as illustrated herein.

3. PURPOSE OF THIS POLICY

This Policy sets out how the Company collects, uses, discloses or processes certain personal information about you, while you are using Company's official website at www.naga.eu

(hereinafter referred to as the "Website"), the Company social networks whereby we maintain online presences (hereinafter referred to as the "Social Networks"), including any personal data you may provide through this Website and Social Networks when you obtain our services.

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 the Company 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.

We would like to point out that 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: Axon Securities S.A.

Contact Person: Data Protection Officer

Email address: dpo@naga.eu

Postal address: 48 Stadiou Street, 105 64 Athens, Greece

Telephone Number: +30 210-3363800

4. DEFINITIONS

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.
- **'Third party'** means a natural or legal person, public authority, agency, or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
- **'Client', 'you'** means the individual who is subject to the personal data we may collect and process as the Data Controller.
- **'Data Protection Legislation'** means the GDPR and all applicable data protection and privacy legislation in force from time to time including without limitation the GDPR; Law 4624/2019 and Law 3471/2006; all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the Personal Data Protection Authority and/or any other relevant regulatory authority.
- **'GDPR'** means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

5. 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 our Data Protection Officer (DPO) at dpo@naga.eu if you have any concerns.

6. HOW WE OBTAIN PERSONAL DATA/ INFORMATION

- **Directly from you**, when for example when you fill in any forms;
- **Through our website**, when for example you give us your consent to use cookies, or you contact us through the website;
- **Through our correspondence with you** for example if you contact us, or when request information for our products or services or when you submit a complaint or when you respond to any of our surveys;
- **Through third parties;**
- **From publicly available sources.**

7. PURPOSE OF PROCESSING:

- **Service provision** - To provide you with our services and or products as well as information regarding these services and products and in general meet our contractual obligations relating to any products or services you use (for example, trading from your Axon account, withdrawing or depositing any amount in your Axon account with your credit/debit card or otherwise) based on our contractual relationship with you;
- **For customers' management purposes** – to support you as necessary, including notifying you for changes to our products or services about new products that you may be interested in;
- **Advertising** – in case you have provide us with your consent, we will communicate to services and/or products provided by us or by third parties;
- **Security purposes** – to prevent any illegal activities or to protect our legitimate interest, including our initiating legal claims and preparing our defence 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;

  Compliance – to comply with our legal obligations**.** Numerous laws to which we are subject to, as well as specific statutory requirements (such as anti-money laundering

laws, Hellenic Capital Market Commission (HCMC) 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 the Company.

8. WHAT PERSONAL DATA WE COLLECT

If you are a potential client and/or a client and/or a visitor to the website or to the App, the data we process are:

- Name and surname, address, email address and contact details;
- Identification documents (such as a copy of your passport and/or ID and/or your Security Body or Armed Forces identity if applicable);
- Proof of your residential address (for example a utility bill, lease agreement, residence or stay permit);
- Date of birth and gender;
- Practice profession and present profession address (for example employer's confirmation certificate, copy of recent payroll, declaration of employment starting date, professional ID(if any), insurance agency documentation);
- Tax registration number (TIN)
- Occupation and information regarding your source of wealth and source of funds;
- Location data (i.e., your IP address);
- Special categories of data, such as the ethnic origin, criminal record (if this is required by a law);
- Bank account details including IBAN details;
- Information collected from your use of website/app
- Information collected from your use of our products, services, app and other similar technologies, for example technical information, including the internet protocol (IP) address used to connect your computer to the internet, the browser type and version, the

time zone setting, the operating system and platform, the type of device you use, a unique device identifier, mobile network information, your mobile operating system and the type of mobile browser you use etc.;

- Information about your activity when you use our Website/ App. Including information about your visit, including the links you've clicked on, through and from our website or app, 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 the Company's products, details of deposits, deposit methods, details of withdrawal, withdrawal methods, details of your exchange activity through the Company, including the date, time, amount, cryptocurrencies, exchange rate, details of device used to arrange the payment and the payment method used;
- Recording communications (see paragraph 16 below);
- Information collected from your use of our Social Networks and/or Company's social feed (see below);

If the Company requests you to provide it with personal date and you fail to do so, the Company may not be in a position to provide a service and/or enter into an agreement with you, in which case it will inform you accordingly.

If you have not created an account with the Company and request for a Chat session, you will be required to provide your email address, first and last name. Any further personal data (including text, files etc.) that may be provided during the Chat Session will be stored in quality monitoring, training and regulatory purposes.

If you are a corporate client, we are required to collect information related to the legal entity (e.g. corporate and constitutional documents), additional personal information on the shareholders, directors and other officer that we deem as necessary in order to be compliant with our legal and regulatory requirements.

Aggregated data i.e., statistical information. By the word aggregated data, we mean a group of data with which people cannot be identified, for example number of people who visiting

our website during the day.

9. LEGAL BASIS FOR THE COLLECTION AND PROCESSING OF YOUR DATA:

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 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, Hellenic Capital Market Commission (HCMC) 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 the Company.

SAFEGUARDING OUR INTERESTS (LEGITIMATE INTERESTS): We process personal data to safeguard the legitimate interests pursued by the Company. Examples of such processing activities include our initiating legal claims and preparing our defence 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 the firm, 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 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 your given consent at any time, by contacting our DPO dpo@naga.eu. However, please bear in mind that any processing of personal data that took place prior to the receipt of your revocation, will not be affected.

The below table provides in detail the purposes for the processing of your data and the legal basis for such processing:

Purposes:	**Legal base**
Verify your identity	Performance of a contract /contract
Establish your account	Performance of a contract /contract
Provide you with our services including products, administrate your account and provide you with technical support	Performance of a contract /contract
Respond to your inquiries or requests	Performance of a contract /contract
Monitor your trading activity to ensure and/or monitor execution quality.	Performance of a contract /contract
Provide you with customer support services	Performance of a contract /contract
Deal with your complaints	Legitimate interest
Keep you informed about new products and services and tailor this information to your needs and interest unless you decide to not receive such notifications.	Consent
Provide you with information about our partners' promotions or offers which we think you might be interested in	Consent
Ask your opinion about our products or services	Consent
Monitor and improve our Website/ App and products	Legitimate interest
Collect your feedback about our Website/ App and products, including statistics and analytic data	Consent
Records keeping	Legitimate interest

Profiling including automated decision (evaluate your knowledge and experience in the financial products that we offer, as well as your investment objectives including your risk tolerance and financial situation, is used to form your economic profile and confirm our assessment of the degree to which such financial products are appropriate to you)	Legal obligation
Prevent, detect, and investigate illegal activities including Money Laundering and Financing Crimes	Legal obligation

- Should be noted that where we use our legitimate interests as the legal base for the processing of your personal information, we have in place extra measures to ensure that your fundamental rights and freedoms will not be overridden by those interests.
- Where we collect and process sensitive information, we have implemented extra security measures to ensure that your data will be process in accordance with the applicable data protection legislation. Such measures include but not limited to limitation of access and processing, minimisation of collection to what is necessary for the purpose of collection, cryptography. For more information, please see paragraph below (security measures).

Anonymous statistical datasets: We prepare anonymous statistical datasets about our clients' trading patterns:

- for forecasting purposes;
- to understand how clients use Company's products and services;
- to comply with governmental requirements and requests.

These datasets may be shared internally in the firm or externally with others, including non-firm 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.

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 Company clients in that country spend their money with. We'll also provide information about how Company 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 Company client.

10. 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 to comply with our legal obligations in regard to suspected abuse of anti-money laundering rules with any firm entity. Such sharing of data in the firm includes and is not limited to the data and documents collected by the Company for identification purposes.

11. TO WHOM WE MAY DISCLOSE YOUR PERSONAL DATA

- **Affiliates companies** – we may share your data with direct or indirect parent undertakings, including but not limited to the firm as well as any subsidiary and/or any holding company from time to, and any subsidiary from time to time of a holding company of that company.
- **Third parties - service providers** such as Suppliers who provide us with IT or payment and settlement infrastructure services, auditors, financial institutions (EMI, Bank Institutions, Payment Institutions), Trading platforms administration providers, regulators, official authorities, including courts and other government bodies, 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 etc. Also, Law Firms in connection with legal claims and to enforce our rights (and those of clients or others) and Accounting Firms for and book- keeping purposes.
- **Legal successors** - as necessary in connection with the sale or transfer of our business.

Where it is required to disclose your personal data to third parties' processors, we ensure that the relevant provisions of GDPR are respected. Specifically, will share data only with those

processors who has implemented such policies and procedures and have in place specific measures with which they ensure an adequate level of protection as required by the GDPR. We also 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. Finally, where such third parties act as our 'processors', we also have in place the required contractual agreements for the protection of personal information in process.

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
Platform providers	To help us provide trading services to you
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

12. INTERNATIONAL TRANSFERS OF YOUR PERSONAL DATA

We may store or transfer your personal data outside the European Economic Area (EEA) for business and management purposes, for the performance of our contractual obligation owed by us to you, or for the provision of services that you may request from us. 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, unless you have provided us with your explicit consent, we will only transfer your data out of European Economic Area where:

- the European Commission has decided that these countries and/or organisations ensure an adequate level of protection;

- the transfer of data is subject to appropriate safeguards (including but not limited to the binding corporate rules or the European Commissioner Standard Contractual Clauses for the transfer of Personal Data out of EU as set out in the EU. Commission decision 2021/914 or one of the derogations of the GDPR for the transfer of Personal Data applies.

13. ONLINE PRESENCE IN SOCIAL NETWORKS

We maintain online presences in Social Networks to interact with you and, among other purposes, to provide information about our products and services.

We would like to point out that the use of the Social Networks is on your own responsibility. This applies in particular to the use of the social and interactive functions (e.g., commenting, sharing, rating, direct messaging), or when you visit and interact with us through any Social Network or when you use a plugin which redirects you to a specific Social Network. We therefore advise you to carefully read their Privacy Policy and to not visit or interact with us through a Social Network, where you do not agree with their practices regarding the personal data processing.

Furthermore, be noted that these Networks are publicly accessible and, therefore, any personal information, comment, or content you may provide through the Social Networks, may be publicly visible or available. For this reason, we strongly recommend you to be aware of the information you are presented with on these Networks.

Finally, should be stated that this Policy does not refer to the processing by any Social Network. If you wish to manage how your personal data is processed by the relevant Social Network, we

strongly advise you to do so through the respective policies and terms of use of the respective Network.

While operating our online Social Network accounts, we may have access to information such as statistical data about the use of our Social Accounts, which is provided by the Social Networks. You may refer to the list below for details of the Social Network data that we may access as administrators of these social accounts.

- **Facebook and Instagram**

  Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland.

  https://www.facebook.com/privacy/policy/

  https://help.instagram.com/155833707900388
- **Google / YouTube, Google My Business**

  For EEA and Switzerland: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.

  https://policies.google.com/privacy?hl=en-US#intro
- **Twitter/ X**

  Twitter International Unlimited Company, One Cumberland Place, Fenian Street, Dublin 2, D02 AX07 Ireland).

  https://twitter.com/en/privacy
- **TikTok**

  TikTok Technology Limited, 10 Earlsfort Terrace, Dublin, D02 T380, Ireland.

  https://www.tiktok.com/legal/page/eea/privacy-policy/enLinkedIn
- **LinkedIn**

  LinkedIn Ireland Unlimited Company Wilton Place, Dublin 2, Ireland.

  https://www.linkedin.com/legal/privacy-policy

Google My Business

We operate a so-called Google My Business entry. Should you connect with us in this way, we will use the information service offered by Google and the services of Google Ireland Limited, (hereinafter referred to as "Google"), for which you may find more information above. 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. We may also be provided, as the operator of the Google My Business listing, with statistical information about the use of Google services. 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.

Should be noted that the data collected about you in this context will be processed by Google and may be transferred to countries outside the European Union. 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. The use of this service is subject to the Google Privacy Policy, which you have already agreed to. You may find more information about how Google processes personal data in Google's privacy policy, as mentioned above.

14. 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 have been trained on how to use and process personal data according to the provisions of the GDPR and the relevant GR legislation and 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.

Furthermore, we consider the safeguard of the personal data by design and by default. This means that we have implemented the appropriate technical and organisational measures to comply with the principles of the GDPR and to secure the confidentiality of the information we hold about you, such as encryption of data, pseudonymisation of data, backups ensuring the

restoration and availability of data and additional evaluation of the effectiveness of the measures in place. Finally, we continually balance the risks for your rights and freedoms through the management risk assessments, while we assess our measures from time to time.

Details of these measures may be available upon request at dpo@naga.eu and to the discretion of the DPO.

15. AUTOMATED DECISION-MAKING AND PROFILING

The Company is assessing your knowledge and experience and is also obliged to assess 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 related Circulars, guidelines and or Regulations or Directives on this matter. For this processing we use the **Appropriateness questionnaire.**

The Appropriateness Questionnaire occurs once you register as a client at the Company where we need to check and ensure that you are suitable for the provision of services and products we offer. This is an evaluation test 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 both suitable for you and in our best of interests.

For this purpose, we may 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:

- Before entering into a contract with you;
- 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 18) below.

We assure you that axon 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 Axon and should you need any clarification, you may contact us at compliance@naga.eu.

16. RECORDING 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 the Company 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.

17. STORAGE AND RETENTION OF YOUR PERSONAL DATA

The Company 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 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 five (5) or (7) years in accordance to the anti-money laundering laws and six (6) years in accordance to the taxation laws:

- a copy of the documents we used 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.

Upon termination of this period, the Company will destruct those records since our legal obligation will not apply anymore.

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.

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

18. 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**: the right to be informed of what data we hold about you, how we process this data, the purpose of processing, with whom we may share your data, the purpose, and the legal base for the processing of your data. Be aware that in some circumstances your right of access may be restricted, for example, 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**: you have the right 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:** your right to ask from us to delete or remove personal data where: (i) there is no good reason for us to continue using it; (ii) the processing is based on your consent (permission) and you have now withdrawn that consent; (; (iii) you have objected to us using your personal data and there are no overriding legitimate grounds for the processing; (iv) we have used your personal data unlawfully; (v) the law requires us to delete your personal data. Should be stated 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 for example, you have terminated your agreement with us or closed your Axon account, we may not be able to delete your entire file because our regulatory responsibilities take priority. We will always keep you informed if we cannot delete l your data to the extent that processing is necessary for compliance with a legal obligation to which Nanag.eu is subject, such as the anti-money laundering law;

- **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 and we will inform you about the reasons of such decision.

- **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 this provision does not adversely affect the rights and freedoms of others, and we 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 to the DPO of the Company at dpo@naga.eu and your request will be further handled. Your ability to exercise these rights will

depend on several 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 information we hold about you, or your rights affect the rights and freedoms of others).

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 (within a month) and keep you updated.

19. 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 Authority's Office:

Website: https://www.dpa.gr/

Email: contact@dpa.gr

Address: Kifisias 1-3, P.C. 115 23, Athens, Greece