



To:

ESE Engineering und Software-Entwicklung GmbH
Theodor-Heuss-Straße 9
38122 Braunschweig, Germany
Commercial Register: District Court Braunschweig, HRB 5288
VAT No.: DE 190230746
Tax No.: 14/202/15407
Technical - Heiko Zschenker: +49 174 7389548
Sales - Celina Dinter: +49 175 5777244
Commercial - Heike Drescher: +49 152 22842336
E-mail: order@ese.de

Αριθ. Πρωτ.: 14725
Ημερομηνία: 04/09/2026

Information: Mrs. Zevgara Z.
Tel: +30 214 414 1036

SUBJ.: INVITATION FOR OFFER SUBMISSION, for Technical Assessment of the Automatic Train Protection (ATP) System of the Refurbished 8th-Series Train for Entry into Service on STASY Line 1

REF: 1) MR-425364
2) Financial Commitment Decision No. 2684/02.09.2026 - ADA: Ψ5ΑΨΟΡΛΟ-Η5Κ
3) ESE GmbH Offer No. 1111591, Version 2.0, dated 26.08.2026
4) Articles 328 & 330 of Law 4412/2016, as amended and in force

Following the above-mentioned references, Urban Rail Transport Single-Member S.A. invites you to submit an offer for the technical assessment of the Automatic Train Protection (ATP) system of the refurbished 8th-series train for entry into service on STASY Line 1.

The scope of the services includes the evaluation of the Safety Case for the refurbished train type, the evaluation of the ATP on-board unit hardware and software approval reports, the assessment of the LZB705 M trackside configuration data and safety section calculations, the assessment of interference current measurements, the assessment of static and dynamic test reports for the pilot train, and the preparation of the relevant assessment report in English. The budgeted expense for this service is twenty-nine thousand eight hundred ninety-eight euros (€29,898.00) plus VAT, where applicable, namely seven thousand one hundred seventy-five euros and fifty-two cents (€7,175.52), i.e. total amount thirty-seven thousand seventy-three euros and fifty-two cents (€37,073.52).



The services provided are classified under the following Common Procurement Vocabulary (CPV) Code: 71630000-3 Technical inspection and testing services.

The offer will not be accepted if the above budgeted cost is exceeded.

Please send us by e-mail to kgram@stasy.gr, to the Central Secretarial Department, no later than 09/09/2026 and until 14:00 (Greece time), your offer as described above, valid tax certificate and insurance certificate or equivalent documents issued by the competent authorities of the country of establishment, as well as a solemn declaration to be signed by the legal representative of the contractor in which the following will be mentioned:

A) For Individuals:

I solemnly declare that I have not been irrevocably convicted of any of the offenses of Article 73 paragraph 1 of Law 4412/2016.

B) For Legal Entities:

I solemnly declare, as the legal representative of ESE Engineering und Software-Entwicklung GmbH, that the undersigned and/or any member of the Executive Board has not been irrevocably convicted of any of the offenses of Article 73 paragraph 1 of Law 4412/2016.

While providing the referred services, your company is responsible for the personnel that will be used during the execution and STASY has no obligation or liability for occupational accidents of your personnel, nor for contributions of EFKA or other insurance services.

While providing the referred services, the contractor complies with the environmental obligations, social security and labor law, which have been established by European Union law, national law, collective agreements or international provisions of environmental, social security and labor law, which are listed in Annex XIV of Appendix B.

Payment Method:

ESE will issue monthly invoices based on the actual working hours performed in the project. Invoices will be based upon the scope of work described above and will be due no later than thirty (30) calendar days after invoicing, without deduction. Further expenses, such as travel time and travel costs, if any and only where applicable, will be invoiced separately following prior confirmation by STASY. STASY is liable for the applicable Value Added Tax (VAT) on the payable amounts, where applicable.

For contract award procedures starting from 01.06.2024, contractors must issue an electronic invoice for the departments of the broader public sector, in accordance with the applicable provisions and instructions of the competent authorities (AADE, Ministry of Finance, etc.).



The invoice must have the following information:

Urban Rail Transport Single-Member S.A.

67 Athinas St., Athens 10552

VAT number: 099939745, Tax Office: KEFODE ATTICA

Electronic invoicing code: 1039.E00923.0001

(For information regarding the payment of the invoice, you can contact the Accounting Department at tel.: +30 214 414 1321)

For assignments worth more than €1,000.00, a retention of 0.1% will be made, which is calculated on the value of each payment before taxes and deductions of the initial, as well as each additional contract. In favor of the Single Public Procurement Authority, it is imposed (article 4 of Law 4013/2011 as in force).

As for anything else, the applicable relevant provisions of Law 4412/2016 and, in addition, the Civil Code apply.

ATTACHMENTS:

ANNEX I - PRIVACY POLICY FOR THE AWARD AND PERFORMANCE OF PUBLIC CONTRACTS

ANNEX II - Privacy Policy for the Award and Performance of Public Contracts



URBAN RAIL TRANSPORT SINGLE MEMBER SA

ANNEX I

PRIVACY POLICY FOR THE AWARD AND PERFORMANCE OF PUBLIC CONTRACTS



Privacy Policy for the Award and Performance of Public Contracts

The company **"URBAN RAIL TRANSPORT SINGLE MEMBER S.A.", trading as "STASY"**, located at 67 Athinas Street, Athens (PC 10552), TIN 099939745 assigned by the tax office KEFODE OF ATTICA, legally represented, respects the privacy and personal data of the Subjects and ensures that it is in a position of continuous compliance with Regulation 2016/679 (EU) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, entitled "General Data Protection Regulation" (GDPR), Law 4624/2019 and the applicable legislation on personal data protection, and to demonstrate such compliance.

With this Privacy Policy for the Award and Performance of Public Contracts, STASY, as the Data Controller, informs the participants in the award procedure, tenderers, economic operators, contractors of public contracts and any third parties involved in the public contract (partners, subcontractors, third economic operators of tenderers and contractors) of the type of personal data it collects, the way in which such data is processed, as well as the protection of personal data.

The Policy applies to all Data Subjects, i.e. all participants in the Tender, economic operators submitting their tender, contractors awarded the public contract and any third parties involved in the public contract. Where the above-mentioned parties are legal persons, the processing of the personal data of such natural persons (legal representatives, shareholders, members, employees, collaborators, persons appointed for the implementation of the contract, etc.) is included.

The Policy applies to all public contracts, public contracts for projects, services, supplies, studies, technical and other related scientific services, general services, as defined in Law 4412/2016, and to all personal data processed on behalf of STASY SA, by any means and in any form.

1. STASY as Contracting Authority and Data Controller

STASY, as the Data Controller, is responsible for and able to demonstrate its compliance with the principles of personal data protection, as well as its general compliance with the applicable legislation on personal data protection.

STASY undertakes that personal data are collected and processed objectively, lawfully and transparently, for a specific and defined purpose, and that the processing takes place in strict compliance with the Privacy Policy of STASY, the provisions of the GDPR, the applicable legislation on the protection of personal data and the Directives of the Personal Data Protection Authority (DPA).



STASY ensures that it processes only the appropriate, relevant and strictly necessary personal data for the purpose for which they were collected and no personal data will be collected or retained for any future use, unless they relate to instances where STASY SA has a legitimate interest in doing so. Staff shall process personal data only for legitimate business purposes directly related to the performance of their duties.

2. Personal Data collected by STASY

As the Contracting Authority, STASY collects, indicatively and not restrictively, the following personal data for the conduct of the award procedure (competitive or not) and the award and execution of the public contract, as provided for by Law 4412/2016, such as: full name, father's name, mother's name, identity details, date of birth, TIN-Tax Office, SSN, contact details, telephone number, address, email address (email, fax), details of scientific training or professional activity, diplomas, work-operating license, start of business at the Tax Office, the supporting documents required by Law 4412/2016 to establish that the reasons for exclusion do not exist, extract from the criminal record, certificates of non-bankruptcy, bankruptcy proceedings, reorganization, etc., tax and insurance clearance, bank account number, IBAN.

The collection of personal data is carried out immediately and directly by the Data Subject (the participant in the Tender, the tenderer economic operator and the contractor) when expressing interest in participating in the procedure, when submitting a tender, by completing all the required supporting documents and submitting the relevant supporting documents on the basis of the provisions set out in the Tender Document or in the instructions for conducting the participation and award procedure, when assigning and awarding the contract and during the performance of the contract. Personal data may also be collected which are manifestly derived from published information or which can be lawfully found and obtained from public authorities.

Personal data provided with supporting documents by the tenderer, in addition and on its own initiative, and which may contain simple personal data or personal data of a special category, are understood to be provided by the Subject with its explicit, free and fully informed consent, knowing that they are submitted for processing for the purposes for which the above personal data are collected.

3. Purposes and Legal Basis of Processing

STASY processes personal data only for the purposes for which the Data Subject was previously informed and does not use them for other purposes that are not compatible with the original purposes.

STASY may process the personal data of the Subject for the purposes listed below, indicatively and not restrictively:



- For the evaluation of the participant, in accordance with the provisions of Law 4412/2016;
- For communicating with and providing information to the participant (e.g. regarding the evaluation of the tender, the delivery of necessary documents, etc.);
- For the award of the contract to the contractor, the performance of the contract, as well as the implementation and support during the performance of the contract;
- For archiving purposes;
- To fulfil the legal obligations of STASY;
- To fulfil the contractual obligations of STASY;
- To defend the rights and legitimate interests of STASY;
- For the general security and protection of transactions.
-

STASY ensures that the processing of personal data is lawful and undertakes to use personal data exclusively and only if there is at least one legal basis that allows the processing of personal data, as follows:

STASY processes personal data under Law 4412/2016, as a Contracting Authority, which, in the exercise of public authority, carries out the procedure for the award of a public contract and supervises the execution and implementation of the contract.

At all stages of the award procedure as defined in Law 4412/2016 (pre-contractual - contractual stage), STASY processes personal data for the evaluation of the participants' data (in the procedure up to the award and conclusion of the contract) and for the control and supervision of the compliance with the contractual obligations arising from the contract.

STASY may process personal data for the fulfilment of a legal obligation, in particular under the provisions of Law 4412/2016, for the fulfilment of a contractual obligation, for the fulfilment of a duty in the public interest, in this case to ensure the transparent conduct of the award procedure, and for serving its legitimate interests.

The Data Subject, by participating and by subsequently being awarded and executing the contract, is deemed to have consented to the processing of its data by providing explicit free and informed consent to the processing.

4. Data Retention- Data Storage- Protection Measures

STASY retains personal data only for the period of time required for the legitimate business purposes for which they were collected, including the purposes of satisfying legal, tax, accounting requirements. Each organisational unit of STASY shall ensure that it identifies and maintains appropriate retention periods and ensures their safe destruction when the period of time has elapsed or the purpose of processing ceases to exist and there is no legal requirement or legitimate interest or right to continue their retention. They may be stored

for a longer period of time if the personal data will be processed exclusively for archiving purposes in the public interest, for scientific and historical research purposes or for statistical purposes and always subject to the application of appropriate technical and organisational measures.

On expiry of the period of time defined either by the contractual relationship with the Subject or by legislation, the procedures for their safe destruction are followed.

5. Instances of Transmission- Disclosure of Personal Data

STASY may disclose personal data to third parties, such as:

- Third natural or legal persons to whom STASY entrusts the performance of specific actions on its behalf and who act as processors (e.g. partners, consultants, etc.);
- The State, public bodies and competent authorities or judicial bodies, within the scope of their powers;
- Participants in the award procedure, within the framework of the principle of transparency and the right to judicial protection of participants, in accordance with the law.

STASY checks and evaluates the processors and requests appropriate safeguards and assurances that they are in compliance with the GDPR and the applicable legislation on personal data protection and that they have taken appropriate technical and organizational measures to ensure compliance. Attached is Annex I - Personal Data Processing Agreement with the processors.

STASY ensures that all its organisational units and its staff (e.g. employees, contractors, assistants, etc.), as well as the processors, are informed of their obligations for the processing of personal data and for compliance with the Privacy Policy of STASY for the management and protection of personal data. At STASY, all staff are responsible for supporting compliance with this policy.

6. Technical and Organisational Data Protection Measures

Taking into account the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, STASY shall implement appropriate technical and organisational measures in order to ensure and demonstrate that the processing is carried out lawfully and provides an appropriate level of data security against the risks involved in the processing.

STASY has drawn up Policies and Procedures for the processing and protection of personal data and has adopted the appropriate technical security measures - for digital and physical security - ensuring the confidentiality, integrity and availability of data.



STASY makes every effort to use the latest technological solutions and procedures for the protection of personal data and to adopt the best protection practices.

7. Personal Data Breach Incident

STASY has established the appropriate structure and procedures to manage any incident related to the processing of personal data. Its staff have been briefed to report any incident that has or may result in loss, theft, unauthorised disclosure, accidental destruction or disclosure of personal data, in accordance with the prescribed data breach response procedures.

In the event of a potential breach, the persons concerned by this Policy are obliged to notify STASY immediately of the incident and to provide any necessary and/or helpful information to deal with the incident. It is stressed that it must be checked whether the breach was caused by their own responsibility and they must also notify STASY accordingly.

8. Consent of the Data Subject

The Data Subject gives consent to the processing of its personal data, after being informed of the purpose of the processing and its rights, by statement or clear affirmative, free, specific, explicit and fully informed action, by which it expresses its consent to the processing of its personal data.

The Data Subject can easily and freely withdraw its consent at any time. The withdrawal of consent shall apply to future processing and shall not affect the processing which was carried out on the basis of the Data Subject's consent prior to the withdrawal and which is lawful processing.

9. Rights of the Data Subject

STASY informs Data Subjects about the processing of their data and the possibility of exercising their rights, and manages the Data Subjects' requests in the best possible way in order to meet the maximum possible degree of satisfaction.

Data Subjects have the following rights regarding the way their data are processed by STASY:

- 1) **Right to be informed** about the processing of personal data;
- 2) **Right to withdraw consent** for data processing at any time;



3) **Right of access** to their personal data. Subjects may request access to their data in order to obtain a copy of the data;

4) **Right to correct**-update their personal data so that the information is accurate;

5) **Right to delete** their data. Subjects may request the deletion of their data in the following instances. Where a) they are no longer necessary for the purposes for which they were collected or processed; b) the consent has been withdrawn; c) there is no longer any legal basis for processing by STASY and processing has no other legal basis. It is emphasised that STASY may not satisfy the right of deletion for reasons of fulfilling its legal obligation, for reasons of public interest, for the establishment, exercise and support of its legal claims, as well as for archiving and statistical purposes.

6) **Right to restrict the processing** of personal data. In this case, STASY shall proceed to the immediate restriction of data processing, at least to examine the restriction request. If the restriction of processing is not feasible, a reasoned reply will be given to the Subject.

7) **Right to data portability**. The Subject may receive in a readable format in one of the widely used reading formats (e.g. XML file) a copy of their personal data processed by computer systems.

8) **Right to object**. The Data Subject may raise an objection to the processing of its data. It is stressed that STASY may not satisfy the right of objection if there is a compelling and legitimate reason, which overrides the request for objection or a purpose for the establishment, exercise or support of its legal claims.

The Subject exercises the above rights by submitting a relevant request to STASY. The request must be clear and specific and as complete as possible so that it can be assessed and satisfied. It must also identify the Subject and confirm its data. STASY shall endeavour to respond within one month to any such request, unless for objective reasons more time is needed, in which case it shall notify the Subject accordingly. A suitable form for completing the request is provided on the website of STASY, www.stasy.gr

In order to exercise any right, the Data Subject may contact the Data Protection Officer of STASY by e-mail at dpo@stasy.gr.

In any event, the Data Subject also has the **right to lodge a complaint** with the Data Protection Authority - DPA as follows: Postal address: 1-3 Kifissias Street, PC 115 23, Athens, Greece; Tel: +30-210 6475600, Fax: +30-210 6475628, www.dpa.gr.

10. Contact



For any information, assistance regarding the exercise or understanding of the Subject's rights and questions regarding personal data, this Policy and the protection of personal data, you may contact the Data Protection Officer of STASY by e-mail at dpo@stasy.gr



ANNEX II:

PERSONAL DATA PROCESSING AGREEMENT

1. INTRODUCTION

1. This Personal Data Processing Agreement (hereinafter the "**Agreement**") is an annex to and an integral part of the contract concluded between the above parties (hereinafter "**Master Contract**"), the parties being, on the one hand, the Societe Anonyme "URBAN RAIL TRANSPORT SINGLE MEMBER S.A.", trading as "STASY", hereinafter referred to as the "**Controller**", and the other hand, the other contracting party, hereinafter referred to as the "**Processor**".

2. In the context of the "**Master Contract**", the "**Controller**" may disclose, communicate or transmit to the "**Processor**" information that constitutes personal data, as defined in Regulation 679/2016 (EU) "General Data Protection Regulation" (GDPR) and the applicable legislation on the protection of personal data (hereinafter "**Law**"), for the purpose of performing the "**Master Contract**".

3. Similarly, the "**Processor**" has the right to process personal data, which are disclosed, communicated or transmitted by the "**Controller**" on behalf of the latter, for the purpose of performing the "**Master Contract**".

4. This "**Agreement**" specifies the terms and conditions of the processing of personal data by the "**Processor**" on behalf of the "**Controller**" and provides appropriate safeguards and assurances that the "**Processor**" is in compliance with the "**Law**".

2. PERSONAL DATA PROCESSING

1. The "**Processor**" shall process the personal data, on behalf of the "**Controller**", which are strictly necessary for the performance of the "**Master Contract**", as well as such data as may be subsequently agreed upon to serve the purpose of the processing. Any such subsequent agreement shall only be accepted in writing and shall be subject to the provisions of this "**Agreement**".

2. In the event that the "**Controller**" in any way discloses, communicates or transmits to the "**Processor**" personal data which are not strictly necessary for the performance of the "**Master Contract**", the "**Processor**" is obliged to notify the "**Controller**" and then proceed to their safe and definitive destruction/deletion.

The "**Processor**" processes, indicatively and not restrictively, the following personal data: personal identification data (full name, father's name, etc.), contact data (telephone number, e-mail address, etc.), etc. Subjects of personal data may include, but are not limited to, the

following persons: employees, passengers, partners, consultants, suppliers, board members of the "**Controller**".

3. The "**Processor**" mainly processes simple personal data, while in special cases, depending on the "**Master Contract**", it may also process special category data, exclusively for the processing purposes as defined in the "**Master Contract**".

4. The "**Processor**" processes the above personal data for the purposes and subject matter of the "**Master Contract**", i.e. exclusively and only for the performance of the assigned activity and the fulfilment of its contractual obligations and for the term of the "**Master Contract**".

5. In case the "**Processor**" has the right to process personal data for additional purposes, as provided for by the "**Law**", they should notify the "**Controller**" before carrying out any processing of the data.

3. OBLIGATIONS OF THE PROCESSOR

1. The "**Processor**" processes only the strictly necessary and necessary personal data and only for the above mentioned processing purposes and in accordance with the instructions of the "**Controller**".

2. The "**Processor**" shall ensure that the persons authorized by them to process the personal data as described above (such as employees, partners, consultants, assistants, assistants, contractors, third parties involved in the "**Master Contract**") are bound by confidentiality terms and clauses and are aware of the terms of this "**Agreement**" and are bound by it accordingly.

3. The "**Processor**" is prohibited from delegating the processing to another processor unless it has previously clearly informed the "**Controller**" to this effect, has committed that the other processor is also in compliance with the "**Law**" and the terms of this Agreement and has received express specific written authorisation from the "**Controller**" to delegate the processing to another processor. The "**Processor**" shall remain fully accountable to the "**Controller**" for the fulfilment of the other processor's obligations.

4. The "**Processor**" is responsible for and must be able to demonstrate its compliance with the "**Law**" and undertakes that the principles of personal data protection and in general the provisions of the "**Law**" are respected for the processing of data carried out by it in the context of the "**Master Contract**".

5. The "**Processor**" shall take all necessary measures to ensure the security of the processing, as well as all appropriate technical and organisational measures to protect personal data.



6. The "**Processor**" shall keep a record of processing activities, separate for all processing carried out for the "**Controller**", which shall be available to the latter upon request.
7. The "**Processor**" is obliged to assist and provide any useful information or best practice to the "**Controller**", so that the latter complies with the obligations under the "**Law**" on the security of processing and the protection of personal data.
8. The "**Processor**" is obliged to cooperate with the "**Controller**" for the management of the requests of the subjects in the exercise of their rights under the "**Law**", for the management of any requests of the Personal Data Protection Authority in the exercise of its duties or for any consultations, for the carrying out of any impact assessment and in general for the protection of personal data.
9. The "**Processor**" is obliged to immediately notify the "**Controller**" if they become aware that any processing operation does not comply with the terms of the "**Agreement**" and the provisions of the "**Law**" and to take any lawful action indicated to immediately remove it.

4. OBLIGATIONS OF THE CONTROLLER

1. The "**Data Controller**" under this "**Agreement**" declares and undertakes that it will process personal data of the "**Processor**" only to the extent that the data is necessary for the fulfilment of the mutual obligations in the performance of the "**Master Contract**" and only to the extent necessary to comply with the legal obligations.
2. The personal data processing carried out takes place in strict compliance with the "**Data Controller's**" Privacy Policy and the "**Law**".

5. TECHNICAL AND ORGANISATIONAL MEASURES

1. The "**Processor**" expressly and unconditionally declares that it applies all appropriate technical and organisational measures in order to ensure the appropriate level of data security and protection, taking into account the type of data, the nature and purposes of the processing and the existing risks of varying probability and severity for the rights and freedoms of natural persons, in accordance with the latest technological - scientific developments and the cost of implementing the measures.
2. The "**Processor**" shall take appropriate technical and organizational measures to ensure that only its authorized personnel have access to the data and the possibility of processing.



3. The "**Processor**" shall take measures to ensure that any natural person acting under its supervision who has access to personal data processes them only in the context of the performance of the "**Master Contract**".

4. The "**Processor**" shall provide the "**Controller**", upon the latter's written request, with all information and evidence of the technical and organisational measures it has taken, and shall allow and facilitate an audit to enable the "**Controller**" to assess the measures to ascertain the level of security and their adequacy.

6. RIGHTS OF SUBJECTS - MANAGEMENT OF REQUESTS

1. The "**Processor**" shall assist the "**Controller**" as far as possible, so that the latter can respond to the requests of the data subjects in the exercise of their rights under the "**Law**". In particular, in the event that the data subject submits any request - a request to exercise a right or a query to the "**Processor**", the "**Processor**" is obliged to notify the "**Controller**" immediately and to forward the request or query to the "**Controller**" as soon as possible and preferably within the next seventy-two (72) hours.

2. The "**Processor**" is not allowed to take any action on its initiative, and in particular is not allowed to manage a request for rectification, erasure or restriction of processing, except on the basis of written instructions from the "**Controller**", unless this is required by the execution of the "**Master Contract**" or required by "**Law**".

3. The "**Processor**" shall ensure that the above shall also bind the persons authorised by him/her (such as employees, partners, consultants, assistants, contractors, third parties involved in the "**Master Contract**"), who process the personal data and may be subject to corresponding requests or questions about the data.

7. CASE OF BREACH INCIDENT

1. The "**Processor**" undertakes that it has included in its appropriate technical and organisational measures the policy for managing and responding to a breach and has informed its staff and other persons authorised by it, so that they can respond immediately to any breach.

2. The "**Processor**" is obliged to immediately notify the "**Controller**", in writing and within the next twenty-four (24) hours, as soon as it becomes aware of a personal data breach, i.e. a breach of data security, which leads to possible, accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of the data or possible, accidental, unauthorized, or unlawful access to the data.

3. The "**Processor**" must, immediately and at its own expense, investigate the breach and act, to the extent possible, to prevent further breaches and implement corrective measures.



4. The "**Processor**" is obliged to notify the "**Controller**" without delay of both the incident and its actions, providing all available information. In particular, it shall provide the "**Data Controller**" with a detailed description of the security breach, the type of data that was the subject of the security breach and the identity of each data subject whose data have been affected, as soon as this information is collected or otherwise made available, including periodic updates of this information and any other information that may be requested in relation to the security breach incident.

5. The "**Processor**" shall assist the "**Controller**" in the notification and communication of the breach incident under the "**Law**" and in cooperation shall take all necessary steps to restore security and enhance data protection by appropriate technical and organizational measures, in order to limit the risk of adverse effects on the rights and freedoms of the data subjects, as well as to mitigate the adverse consequences and limit as far as possible the risk of future breaches.

6. With regard to the obligation to notify the "**Controller**" immediately and in writing, this applies even if the "**Processor**" has doubts as to the security or lawfulness of the processing. In this case, they must refrain from processing and notify the "**Controller**" immediately.

8. DATA RETENTION; RETURN AND DELETION OF DATA

1. Throughout the term of the "**Master Contract**", the "**Processor**" confirms that it has taken appropriate technical and organisational measures to protect the personal data and that it maintains the data by ensuring their confidentiality, integrity and availability.

2. After the termination of the "**Master Contract**", within a reasonable period of time, which may not exceed fifteen (15) calendar days, the "**Processor**" shall return to the "**Processor**" all documents in its possession and all work products and data produced and delete any personal data file it has created and maintains for the purposes of this Agreement, forwarding to the "**Processor**" the relevant deletion protocol.

9. DATA TRANSMISSION

1. The "**Processor**" shall not transmit to recipients and third parties the personal data provided by the "**Controller**". The possibility of transfer is provided for in the case of the fulfilment of a request from a data subject, following an instruction from the "**Controller**" and in the case of a request from the "**Controller**" itself for the provision and/or return of the data.



2. In case the transfer of data results from a legal obligation of the "**Processor**", before carrying out any processing, he/she is obliged to notify the "**Controller**" about the terms and obligations of the transfer.

3. The "**Processor**" processes personal data exclusively within the territorial limits of the European Union (EU). Any transfer of data requires prior notification and written consent of the "**Controller**". Such transfer is subject to compliance with the specific requirements concerning the transfer of personal data under the "**Legislation**".

10. CONFIDENTIALITY - OBLIGATION OF SECRECY

1. Throughout the term hereof, and after its expiration or termination, the "**Processor**" undertakes to keep confidential and not to disclose, share, publish, announce or otherwise disclose to third parties, without the prior written consent of the "**Processor**" any documents or information and all or part of the data that have come to its knowledge in the course of fulfilling its obligations and providing its services in the performance of the "**Master Contract**".

2. The "**Processor**" is obliged to keep as highly confidential any data received from the "**Controller**" for the performance of the "**Master Contract**", as well as not to use them for any other purpose than the one specified herein.

3. The provisions of this Article shall be binding on the "**Processor**" even after the termination or cancellation of this Agreement in any way.

11. BREACH OF THE TERMS OF THIS AGREEMENT

1. The "**Processor**" processes the personal data on behalf of the "**Controller**" and does not exceed the limits of the instructions given by the latter regarding the purposes and processing of the data under the "**Law**". In the event of exceeding the limits and action of the "**Processor**" beyond the purposes of the "**Master Contract**" and this Agreement, the "**Processor**" shall be understood as the "**Controller**" for any processing it carries out, setting itself the purpose and means of processing the data, and shall bear the responsibility and consequences of the "**Law**".

2. The "**Processor**" is fully liable to the "**Controller**" for any direct, indirect, present, future, positive or consequential damage to the latter due to the breach of the obligations and terms of the "**Agreement**". The same liability shall apply to the designation of another processor and its breach of the obligations and conditions of the "**Agreement**", without limiting any right of the "**Controller**" to take action against the other processor in the same way.



3. Breach of any term hereof constitutes a material breach of the "Master Contract".

-----END OF TEXT-----



Spyridon Bratsos

Διευθυντής Προμηθειών & Ανεφοδιασμού ·