# DATA PROCESSING AGREEMENT (hereafter the Agreement)

In Thessaloniki today on [date] between the Contracting Parties:

1. **…………….** on behalf of **Aristotle University of Thessaloniki (AUTH)** located in University Campus, 54124(hereafter the Controller) and
2. [full name] (hereafter the Processor)

collectively referred to as the “Parties”,

**PREAMBLE:**

**Considering that:**

1. The Parties have already signed an agreement on the [date] (hereafter the “Main Contract”), which concerns [subject-matter of the contract]. This Agreement constitutes the Annex to the Main Contract.
2. On 25 May 2018 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) entered into force (hereafter the Regulation)
3. The controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, who determines the purposes and means of the processing of personal data as well as processes the personal data
4. The processor is a natural or legal person, public authority, agency or other body who processes personal data on behalf of the controller and in accordance with the instructions of the controller
5. The Controller and the Processor are required to comply with the Regulation, to the respective European and Greek law concerning the protection of natural persons regarding the processing of personal data and the handling of information classified as Secret as well as to the Decisions, Guidelines and Opinions issued by the Hellenic Data Protection Authority.
6. The controller has already entrusted/will entrust the processor with the processing of personal data on behalf of the controller according to the Main Contract and specifically according to the main Contract, which was signed on [date].

**The Parties already herewith acknowledge, agree and accept the following:**

**1. DEFINITIONS:**

Under the legislation governing the processing of personal data [General Data Protection Regulation 2016/679 EU (hereinafter Regulation) and national legislation ............] and for the purposes of this Agreement, the basic concepts used are:

**“Personal data”** means any information relating to an identified or identifiable natural person (‘data subject’); 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;

**“Data of special categories or sensitive personal data**” comprise personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, register of criminal convictions and offences.

Health Data refers to information relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status; Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected when enrolling for health care services and during the provision of health services as referred to in Directive 2011/24/EU of the European Parliament and of the Council. Such information may be a number, symbol or identity item attributed to a natural person for health purposes, information resulting from tests or analyses on part of the body or body substance, including genetic data and biological samples; and any information about, for example, a disease, disability, disease risk, medical history, clinical therapy or the physiological or biomedical condition of the data subject whatever its source, for example by a doctor or other healthcare professional, a hospital, a medical device or an in vitro diagnostic test.

 **“Data subject”:** an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identity number, location data, an online identity card or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

**‘Processing’**: any operation or set of operations carried out with or without the use of automated means on in personal data or in sets of personal data such as the collection, registration, organisation, structure, storage, adaptation or alteration, retrieval, retrieval of information, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, restriction, erasure or destruction;

**“Controller”:** the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

**“Processor**”: a natural or legal person, public authority, service or other entity processing personal data on behalf of the controller;

**“Subcontractor”**: a natural or legal person who is entitled by the Processor to process personal data on behalf of the Controller in the context of the main contract;

**“Personal data breach”:** a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed;

**“Main Contract” (when reference is made in this Agreement or in the main contract):** one or more contracts signed or scheduled to be signed in the future between the controller and the processor and their subject-matter concerns the subcontracting of provision of services to the processor entailing the processing of personal data.

**2. PROCESSING OF PERSONAL DATA**

2.1. The processor processes the personal data on behalf of the controller based only on his written orders as defined in the main contract and this Agreement. Processing by a processor shall be governed by this Agreement that is binding on the processor with regard to the controller.

2.2. These orders are written and refer especially to the subject-matter, purpose, nature and the duration of the processing as well as to the type of personal data, the categories of the data subjects concerned and the obligations and rights of the controller and may be given on one-off basis or on a case by case basis either in the main contract or in an annex thereto. [[1]](#footnote-1)Εναλλακτικά: *Οι εντολές αναφορικά με το αντικείμενο, τον σκοπό, τη φύση και τη διάρκεια της επεξεργασίας περιλαμβάνονται στο παράρτημα…. της παρούσας/ του παρόντος.*

2.3. These orders are subject to change by the controller after timely notification of the processor, in case it is necessary to adjust the processing of personal data he performs on behalf of the controller.

2.4. The processor processes personal data in the context of the (main) contract concluded with the controller and for the purposes of the provision of the agreed services between the controller and the processor. Any other processing of personal data in any way and form is not allowed unless such processing is necessary to comply with a legal obligation of the processor. In this case, the processor shall inform the controller of the legal claim in question before processing unless such information is prohibited by law for serious reasons of public interest.

2.5. The processor undertakes to inform the controller in advance and in due time if a personal data transfer to a third country or international organization is necessary unless such briefing is prohibited by law for serious reasons of public interest. Prior to this transfer, the processor undertakes to ensure that adequate safeguards are in place to protect personal data (e.g. transmission in accordance with the adequacy decision issued by the European Commission, conclusion of standard contractual clauses approved by the European Commission, a code of conduct or a certification mechanism approved by the European Commission, etc.). The controller has the right to oppose to such a transmission, unless required by law.

2.6. If the processor exceeds the orders received by the controller and determines the purpose and means of processing the personal data on his own initiative or processes them for purposes other than the specified purposes, the processor shall be considered to be the controller in respect of that processing and has the respective obligations and responsibility towards data subjects and supervisory authorities, irrespective of his responsibility towards the controller.

**3. PROCESSOR’S STAFF AND RECRUITMENT OFANOTHER SUBPROCESSOR**
3.1. The processor informs the authorized persons to process personal data about the obligations arising from the legislation and this Agreement.

3.2. The processor ensures that the authorized persons process personal data only on documented instructions from the controller including with regard to transfers of personal data to a third country or an international organisation unless required to do so by Union or Member State law to which the processor is subject; in such a case the processor shall inform the controller of that legal requirement before processing unless that law prohibits such information on important grounds of public interest. The processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or under an appropriate statutory obligation of confidentiality obligation.

3.3. The processor ensures that only the authorized persons, as appropriate and for the purpose of the processing, have access to personal data and only for the agreed purpose of the processing.

3.4. The processing shall not engage another processor ("subcontractor") without prior specific or general written authorisation of the controller.

Alternatively (general permission with a right to object): The processor is entitled to recruit another processor ("subcontractor") but informs the controller in due time and in detail of any intended changes regarding the addition or replacement of the other processors. The controller is entitled [within ... working days] to oppose, in whole or in part, to the recruitment or replacement of subcontractors.

3.5. The processor ensures and guarantees that the subcontractor shall be governed by law and this Agreement and is able to meet the requirements of the processing of personal data arising from the main contract and this Agreement. Upon the request of the controller, the processor shall notify him of the terms of the contract he is about to conclude with the third party/ subcontractor and shall, where appropriate, communicate a copy to the controller, without prejudice to its confidential content, which, however, shall not render meaningless the terms of processing of personal data as laid down in the main contract and this Agreement

3.6. When the subcontractor is unable to meet his obligations regarding data protection, the processor remains fully accountable to the controller for the fulfillment of the subcontractor's obligations.

**4. DELETION / RETURN OF PERSONAL DATA TO THE CONTROLLER**
4.1. After the main contract has been terminated for any reason or after completion of the processing that has been assigned to the processor by the controller, the latter shall declare to the processor if he shall:

(a) delete the personal data; or

(b) return all the personal data to the controller.

4.2. The processor shall ensure that the subcontractors are informed of the choice of the controller as well as ensures that they comply with it.

4.3. The processor and, where applicable, the subcontractor shall delete existing copies within ten (10) days unless Union or Member State law requires storage of the personal data. In this case the processor shall inform the controller accordingly. Personal data are kept separate and subject to organizational and technical security measures. Their processing is permitted only for the purpose for which they are lawfully maintained.

**5. RECORDS OF PROCESSING ACTIVITIES**

5.1 The processor keeps a record of all categories of processing activities carried out on behalf of the controller.

*5.2. This record shall include at least the following:*

(a) the name and contact details of the processor and of each controller on behalf of which the processor is acting works and, where appropriate, of the of the controller’s or the processor’s representative,

(b) the name and contact details of the Data Protection Officer, where designated

(c) the categories of data subjects and the categories of personal data and of processing carried out on behalf of each controller

(d) a general description of the technical and organizational security measures.
(e) where applicable, transfers of personal data to a third country or an international organisation including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards

5.3. The processor keeps records of processing activities in writing and in any case in electronic form. The executor is required to keep the relevant records up to date and adds or removes processing activities and related information as appropriate.
5.4. The processor places the processing activity file at the disposal of the controller upon his request. The controller reserves the right to request specific explanations from the processor regarding the content of the processing activities archive as well as propose reasonable modifications and additions with the view to achieving fuller and more effective compliance with all obligations under the Regulation and this Agreement.
5.5. The processor and, where applicable, his representative shall make these records available to the Data Protection Authority upon request.

**6. OBLIGATIONS REGARDING THE PROVISION OF ASSISTANCE IN ENSURING COMPLIANCE WITH THE GDPR**

6.1 The processor shall provide assistance in ensuring compliance with the GDPR in particular to ensure compliance with the obligations under the Regulation and the applicable law. This obligation includes the processor’s assistance when deemed necessary in order to enable the controller to respond to queries, complaints and requests related to the exercise of rights of data subjects.

6.2. The processor shall provide his / her assistance regarding the exercise of the following rights of the data subjects: information, access, rectification, erasure, restriction of processing, data portability and objection to processing.

6.3. The processor shall immediately / without undue delay inform the controller in writing or in any other appropriate manner that has been agreed, of any question, complaint or requests related to the exercise of rights received by data subjects.

6.4. Where appropriate, and at the request of the controller, the processor is required to provide his / her assistance in informing the data subjects regarding the granting of the consent and the collection / receipt of the consent.

6.5. The processor is required to provide the controller with assistance in carrying out a data protection impact assessment.

6.6 The processor is obliged to provide the controller with assistance on consulting the Data Protection Authority regarding the proposed and appropriate risk mitigation measures in cases where the impact assessment study indicates that the processing of personal data would cause a high risk for the rights and freedoms of data subjects.

**7. CONFIDENTIALITY, PROTECTION OF PROCESSING AND ASSISTANCE IN PROVIDING NOTIFICATION OF BREACH**

7.1. The processor is committed to the confidentiality of the personal data that he/she processes on behalf of the controller. The processor may disclose personal data to third parties only with the explicit mandate or consent of the controller. The processor may deviate from this commitment only if disclosure is required by a law provision for which the processor is required to inform the controller unless such disclosure is prohibited by law.
7.2. The processor takes particularly into consideration the nature of the processing of personal data and the risks arising from or regarding it such as the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized access to personal data, which could lead to physical, material or non-material damage and takes all necessary measures to prevent them.

7.3. The processor is required to take all appropriate technical and organizational measures to ensure the appropriate level of risk protection including but not limited to: (a) pseudonymisation and encryption of personal data, (b) the possibility of ensuring confidentiality, the integrity, availability and reliability of processing systems and services on a continuous basis, (c) the availability of recovering personal data and the accessibility to personal data in due time in case of physical, material or non-material damage, (d) a procedure for the regular testing, assessment and evaluation of the effectiveness of technical and organizational measures to ensure the safety of processing taking into account the latest developments, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different likelihood of occurrence and seriousness for the rights and freedoms of natural persons. Alternatively: these measures are described in the appendix hereto.

7.4. The processor ensures that from the point of view of expertise, reliability, financial and technical resources, he/she is in a position to take appropriate technical and organizational measures to ensure that the processing is lawful as well as to safeguard the rights of the data subjects and the appropriate level of risk protection. The processor shall be obliged to inform the controller of these measures and allow him to carry out relevant checks to confirm the reception and the adequacy of the technical and organizational measures.
7.5. The processor shall assist the controller in order to comply with the obligations regarding the security of processing.

7.6. The processor is obliged to inform the controller in writing or in the most appropriate manner on a case-by-case basis of each personal data breach and to provide him with all the necessary information (nature of the violation, data categories, estimated number of affected data subjects etc.) on the respond to this personal data breach and the management of related issues. The notification shall be made immediately / without undue delay and no later than twelve hours after having become aware of the personal data breach.
7.7. The processor shall take all necessary measures to limit the breach, keep the controller informed in order to take the necessary measures to deal with the breach of personal data and, where appropriate, mitigate its possible adverse effects.
7.8. The processor shall assist the controller regarding the notification of personal data breaches to the competent Data Protection Authority and the communication of personal data breaches to the data subject.

**8. PERFORMANCE OF OFFICIAL CONTROLS**

8.1. The processor shall make available to the controller any information necessary to demonstrate compliance with the obligations laid down in the Regulation and hereto.
8.2. The processor shall allow and facilitate inspections by the controller, including on-the-spot checks and inspections, cοnducted by the controller or another auditor mandated by the controller.

8.3. The controller shall inform in writing and in due time the processor of his intention to carry out an inspection and shall do so in a manner that does not cause a disproportionate burden on the operation and the activities of the processor.

8.4. The controller and processor are required to assist each other in carrying out inspections and investigations carried out either by the Data Protection Authority or by another authority or courts in compliance with this Regulation or every relevant Law.

**9. RESPONSIBILITY**

9.1. The processor has full responsibility and the obligation to fully compensate the data subject and / or the controller for any damage suffered by him / herself, directly or indirectly, and any third party including the data subjects when the damage was caused as a result of failure to comply with or breach of the legal mandate or instructions given by the controller as well as breach of the present terms of this Agreement and / or the obligations imposed on the processor by the Regulation and the national and European framework for the protection of personal data as a whole.

9.2. The processor has the responsibility and the obligation to compensate the controller for any damage he has sustained by acts or omissions of his staff, officers, representatives or subcontractors who have been entrusted with all or part of the processing.

9.3. The controller or processor is exonerated from his liability if he proves that he is not responsible for the event giving rise to the damage.

9.4. If the controller or processor has paid full compensation for the damage caused to the data subject, the controller or the processor has the right to ask respectively the other processor or controller involved in the same processing, to recover the part of the compensation corresponding to the part of his respective liability due to the damage caused under the conditions of clause 9.1.

**10. ENTRY INTO FORCE- DURATION – END OF AGREEMENT**

10.1. This Convention shall enter into force and produce legal effects from the date of its signature.
10. 2. This Convention shall remain in force as long as the main contract is in force and terminates upon termination of the main contract between the parties.

**11. GENERAL TERMS**

11.1. With respect to any dispute, dispute or claim and for any reason whatsoever arising, including but not limited to disputes concerning the existence, validity, interpretation and termination of this Convention, Greek law is applicable and the courts of Athens are competent except if otherwise agreed in the main contract.

11.2 This Convention does not in any way restrict the obligations of the processor as defined in the main contract nor can it be interpreted as permitting processing in a manner prohibited by the main contract.

11.3 In the event that any term of this Agreement is declared invalid or unenforceable, the remaining terms remain in full force entailing rights and obligations.

Ιn witness whereof, the present Agreement was drawn up in two (2) identical copies, which were signed by the parties after being read and each party received one copy.

THE CONTROLLER THE PROCESSOR

1. Σημείωση : το αντικείμενο της επεξεργασίας και οι οδηγίες του υπευθύνου προς τον εκτελούντα θα πρέπει να ορίζεται είτε στην κύρια σύμβαση είτε να υπάρχει σχετικό παράρτημα. [↑](#footnote-ref-1)