Privacy and data protection policy

PREAMBLE

In accordance with the provisions of 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 (hereinafter "**GDPR**")) on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such Data and Related Legislation, the Mateas Foundation processes personal data in accordance with the principles mentioned below, for legitimate purposes.

The processing of personal data is done by mixed means (manual and automated), in compliance with the legal requirements and under conditions that ensure the security, confidentiality and observance of the rights of the data subjects.

The main objective of this Security Policy is to contribute to the activity of the Mateas Foundation by observing the specific legal provisions and minimizing the associated risks by preventing any incidents and, in the unlikely case of such an incident, the minimization of its impact on the data subject.

We undertake to have a relationship based on trust, transparency, good faith and ethics in relation with all our partners, colalborators, employees and all data subjects whose personal data we process.

Considering Mateas Foundation operates a school and therefore we have access to children data, we have taken increased security measures to prevent any incidents regarding thereof.

1. DEFINITIONS

a) **Personal data**: any information relating to an identified or identifiable individual; 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;

b) **Processing of personal data**: 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;

c) **Storage**: Keeping personal data gathered on any support

d) **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.

e) Processor: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

f) **Recipient:** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

g) **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;

h) **Consent**: means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

2. COMMITMENT OF MATEAS FOUNDATION:

a) Protecting the security and security of processed personal data is especially important not only for the Foundation Mateas but more importantly for the data subjects.

b) The Mateas Foundation will take all necessary technical and organizational measures to ensure an adequate level of protection regarding the processing of personal data in accordance with the provisions GDPR and any other applicable legal provisions.

3. PRINCIPLES OF PERSONAL DATA PROCESSING

a) **Legality, equity and transparency**: Personal data is processed in good faith, under and in accordance with the legal provisions in an equitable and transparent manner towards the data subject in order to protect the fundamental rights of the data subjects;

b) **Well-defined, explicit and legitimate purposes**: Any personal data processing is only done for well-defined, explicit and legitimate, appropriate, pertinent and not excessive purposes in relation to the purpose for which it is collected and subsequently processed;

c) **Information and legal grounds**: By means of this information, individuals become aware of the fact that their personal data will be processed having a well determined legal ground, such as legal provision, the consent of the data subject, performance of agreements and the legitimate interests of the Mateas Foundation (which shall not be opposed to the superior interests of the data subject);

d) **Storage and purpose limitation**: Personal data is not stored for a longer period than is necessary to achieve the purposes for which it was collected and processed in accordance with the data subject's rights provided by GDPR and is only processed if they are adequate and relevant for the legitimate purpose for which they were initially collected or other compatible purposes;

e) **Protection of the data subjects**: The data subjects have the right of access to the processed data, of intervening on them, of the opposition and of not being subject to any individual decision, as well as the right to address to the National Supervisory Authority for Personal Data Processing or Court to defend any rights guaranteed by law that have been violated;

f) **Security**: The Mateas Foundation will take continuous adequate technical and organizational measures of personal data security to prevent the accidental or illegal destruction, loss, modification, disclosure or unauthorized access (access to user databases is based on username and password, regulated by roles and access rights). The possibility of alteration of the accessed data is protected by Mateas Foundation's firewall, as well as permanently updated antivirus solutions.

g) **Accuracy:** Mateas Foundations processes personal data accurately and tales measures to ensure that any incorrect personal data it acknowledges are deleted or rectified.

4, PERSONAL DATA PROCESSING POLICY

In accordance with the provisions of GDPR, the Mateas Foundation has the obligation to manage safely and only for the purposes presented below, the personal data that are provided to it.

The Mateas Foundation undertakes to maintain the confidentiality of the personal data provided as required by the provisions of GDPR.

5. COLLECTED DATA

Depending on each activity, Mateas Foundation may process the following categories of data regarding data subjects:

- Name;
- Contact data: phone, e-mail;
- Identification details, according to the identity card/passport;
- Data on family members, including those of employees for observing the legal provisions in the field of labour law;
- Image and voice of students and employees;
- Professional data: previous workplaces, position, seniority;
- Educational data;
- Certain medical data collected by our on-premises nurses;
- Data regarding criminal antecedents, considering our employees work with children;
- GPS tracking;

These data may be collected from the following sources:

- Public sources;
- External databases – for example, during the recruitment process we conduct a through background check of our candidates;
- Direct provision from the data subjects through e-mail, telephone and, most importantly, forms;
- Agreements;

6. PURPOSES AND GROUNDS FOR PROCESSING

We collect personal data for the following **purposes**:

a) providing the highest quality educational services to children - filling in and managing the database of preschoolers / pupils and potential preschoolers / pupils, for drawing up and issuing graduation/studies certificates / diplomas;

b) promoting our services;

c) performing agreements with suppliers and partners;

d) during human resources processes (e.g. recruitment, payroll).

We collect personal data under the following **grounds**:

a) Consent of data subjects. We have undertaken as a general rule to obtain the written consent of data subjects with their proper information. However, in some cases, we will consider consent as being granted by the simple fact that the data subject shall have the initiative of sending certain personal data to us, for example, in case we are contacted through the e-mail address on our website;

b) Performance of agreements;

c) fulfilling legal obligations – for example, in relation to specific requirements of the Ministry of Education in Romania;

d) fulfilling certain legitimate interests of the Mateas Foundation which shall not be opposed to the superior interests of the data subject.

7. RECIPIENTS

Due to the nature of our business we transfer certain non-sensitive personal data to entities outside the European Union, the most important being:

a) SABIS, a renowned global education network that has an active presence in 20 countries on five continents which is located in the United States and with which we collaborate continuously to ensure compliance with GDPR;

b) The Lebanon Embassy, considering that this is a Lebanon funded organization, and which observes not only the confidentiality provisions under the laws of Romania but also those from Lebanon.

We do not provide third parties personal data for marketing purposes.

Personal data is processed by Mateas Foundation in its capacity as controller and may disclose them only to processors contracted by us and which observe strict security and confidentiality requirements.

We also disclose data to Romanian public authorities, in accordance to the legal provisions in force.

8. DATA SUBJECTS' RIGHTS

In accordance with the provisions of GDPR, the individuals registered as the data subjects have the following rights:

a) **Right to be informed**: the right to find out which data is processed, the purposes and grounds of the processing, recipients of the data, storage period, the rights of the data subject, the right to contact the supervisory authority;

b) **Right to access**: the right to obtain from the operator a confirmation whether personal data is processed or not and, in case the answer is affirmative, access to the respective data and information on the previously detailed processing;
c) **Right to rectification:** the right to obtain the correction of inaccurate data or the supplementing of missing data;
d) **Right to erasure:** the right to request the deletion of processed data, according to the law;
e) **Right to restrict processing:** the right to request the restriction of processing, to the extent permitted by law.
f) **Other rights:** such may be exercised according to the law: right to data portability, right to object to data processing, right to oppose automated decisional processes, right to contact the competent authorities.

9. PERSONAL DATA SECURITY

The Mateas Foundation certifies that it meets the adequate personal data technical and organizational security requirements, as required by GDPR.

Foremost, our activity is based on the principle of preventing any security incidents, such as unauthorized access to data, information leaks, accidental data erasure and other similar incidents.

The Mateas Foundation uses security methods and technologies, along with employee policies and work procedures, including control and audit, to protect personal data collected in compliance with the legal provisions in force.

Collected personal data will only be used for the stated purpose of these security policy guidelines.

However, considering that in no case the security of processing can be 100% guaranteed, Mateas Foundation has taken measures that, in the unlikely case such incidents do occur, their extend and gravity are diminished.

10. SECURITY REQUIREMENTS COVERAGE.

The President of the Mateas Foundation designates by internal decision the Person/s responsible, respectively the users accessing the databases and processing the personal information:

A) User identification and authentication

"User" means any individual acting under the authority of the Mateas Foundation with a recognized right of access to personal data databases.

To access a personal data database, users are required to identify themselves. Identification will be done by entering the identification code from the keypad (one character string). Each user will have their own identification code, distinct from the other users' identification codes.

Any user account will be accompanied by an authentication method. Authentication will be done by entering a password set by each individual user. Passwords will consist of at least 8 (eight) characters consisting of at least 3 of the following four sets of characters: Small, capital letters, numbers or special characters.

Mateas Foundation - Cambridge School of Bucharest
Calea Dorobantilor 39, Sector 1, Bucharest, Romania
Tel: +40 21 210 2131/8 | **Email:** office@cambridgeschool.ro
www.cambridgeschool.ro

The responsible person or the users designated by him / her for this purpose will ensure the revocation or suspension of an identification and authentication code if their user resigns or has been fired, has terminated his/her contract, has been transferred to another service and the new tasks do not requires him/her to have access to personal data, has abused the codes received, or if he / she will be absent for more than 60 (sixty) days.

Any user who receives an identification code and authentication means must keep their confidentiality and will be liable to disciplinary action for any disclosure of this information to third parties due to a faulty action or omission of the user.

The responsible person will agree with the technical department on the procedure of administration / management of user accounts.

B) Type of access:

Users must only access the personal data required to perform their job assignments. The Responsible Person will act personally or designate another person within the Mateas Foundation who will act as **Administrator** of databases compiling personal data (**Database).**
The Responsible Person will determine what the attributions are and what actions can be taken by each user in relation to the Data database (such as reading, collecting, inputting, processing / modifying or deleting personal data from the Data Database).

Programmers of the personal data processing system will not have access to personal data. The Mateas Foundation may decide that programmers have access to personal data, but only to the extent that these data have previously been converted to anonymous data.

The technical support compartment may have access to personal data to resolve exceptional cases.

Anonymous data will be used to prepare users or make presentations. Employees who teach training courses will use personal data during their own training, with strict adherence to legal provisions.

C) Execution of back-up copies

The information system will ensure the execution of backup copies of the Databases as well as of the programs used for automated processing at a reasonable time but in no case longer than 15 (fifteen) days.

The responsible person will authorize a maximum of 3 (three) users to run the backup copies. Backup copies will be stored in a secure server room, different from computer rooms. Access to the secured room will be restricted and allowed to a reduced number of employees of the Mateas Foundation. If it is absolutely necessary for the protection of personal data processed and only to the extent that Mateas Foundation has such spaces, the backup copies will be kept in rooms in another building.

D) Computers and access terminals Personnel training

The computers and other access terminals on which the personal data processing operations will be performed will be installed in restricted access rooms, requiring the use of an access card / keys to enter the room. Access to these rooms of individuals other than authorized users will be only permitted if those individuals are accompanied by the Responsible Person or one of the users designated for this purpose by the Responsible Person. The Responsible Person will ensure that the access of employees / other individuals providing services to the Mateas Foundation (such as cleaning services, utilities, etc.) takes place under the above-mentioned conditions or, if this is not possible, will take reasonable measures to ensure that those individuals are unable to intervene in any way in the processing of personal data during the period in which they are in the room (e.g. by closing the processing session and / or the computers within the area in which the third person has access).

Users are required to lock their working station when they leave the computer on which personal data processing is performed.

E) Personnel training

Prior to the commencement of any processing operation by the users, the Responsible Person will provide their training (personally through other individuals within the Mateas Foundation or third parties with the necessary knowledge in the field) regarding: the provisions of LGDPR, the adequate security requirements for the processing of personal data, as well as the risks involved in the processing of personal data, depending on the specificity of the user's activity, as well as on the confidentiality of the processed data. The information system will also send a message about the privacy of personal data whenever a user accesses the databases.

F) Use of computers

In order to maintain the security of personal data processing (especially against electronic viruses) Mateas Foundation will impose the following measures:

1- Prohibition of the use by software users of software that comes from external or doubtful sources;

2- Information of users about the threat concerning computer viruses;

3- Implementation of automatic debugging and security systems for information systems; Antivirus applications used by the Mateas Foundation are installed and configured by Mateas Foundation's specialized staff and cannot be modified by users. The antivirus server connects to the antivirus solution provider's server and receives updates every hour; updates are then transmitted through the intranet. The antivirus solution used by the Mateas Foundation offers several forms of scanning: (i) manual scanning; (ii) real-time scanning; (iii) scheduled scan once a week; (iy) immediate scanning. If a virus is detected, the file / files will be debugged or quarantined.

The Mateas Foundation may decide to take additional measures for the same purpose.

Mateas Foundation - Cambridge School of Bucharest
Calea Dorobantilor 39, Sector 1, Bucharest, Romania
Tel: +40 21 210 2131/8 | **Email:** office@cambridgeschool.ro
www.cambridgeschool.ro

G) Data printing

The printing of personal data will be only performed by the designated users and only for the purpose specified in these rules.

H) Audio-video monitoring

The technical installation and use of the equipment and components of the audio-video surveillance system is carried out in accordance with the legal regulations in force.

Audio-video surveillance is performed for the following purposes:

1- Preventing and combating offenses;
2- Ensuring the security and protection of individuals, property and values, and the real estate in which the Foundation operates.

Audio-video recordings are stored for maximum 20 days on the central monitoring unit, after which the information is overwritten.

I) Other security measures

We have signed additional documents with our employees, suppliers and partners in order to ensure adequate security for the data we process.

We have implemented physical security measures, such as the storage of documents containing personal data in lockers under key which is available only to specific staff, access card etc.

We monitor our premises continuously in order to prevent and, if the case, identify unauthorized access.

11. FINAL PROVISIONS

For more details and information, any interested person can contact us at our headquarters or by email at joseph.khoury@justentrepreneur.com or by phone at 0726.377.377.

For the exercise of certain rights, we reserve the right to request that the application be submitted in writing, signed by the data subject which may be required to present adequate proof regarding its identity.

Chairman of the Board of Directors,
Mr. El Khoury Joseph