A. 89 Dyrrachiou str. and Kifisou, 104 43, Athens, Greece
T. (+30) 210 3636936
E. office@admieholding.gr
www.admieholding.gr
Registration No: 141287501000

PRIVACY POLITICS AND SECURITY OF PERSONAL DATA

As has been approved by Minutes No. 52 of the Company on June 2nd, 2020

In compliance with the provisions of Regulation (EU) 2016/679

[*on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC* - **GDPR]**

and Law 4624/2019 (A '137)

***This is a translation from the original version in Greek language. In case of a discrepancy, the Greek original will prevail.**

Introduction – Purpose – Content

The protection of individuals against the processing of personal data is a fundamental right. Article 8 par. 1 of the Charter of Fundamental Rights of the European Union stipulates that every person has the right to the protection of personal data concerning him or her. According to par. 2 of the same article, the processing of the data must be done legally, for defined purposes and based on the consent of the interested party or for other legitimate reasons, provided by law. Every person has the right to access the collected data concerning him and to achieve their correction

Furthermore, from 25.5.2018, Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR) of the European Parliament and of the Council enters into force, which introduces a stricter framework for the protection of individuals against the processing of personal data and for the free movement of such data (hereafter referred to as the "General Regulation"). Moreover, as early as August 2019, Law 4624/2019 entered into force, which, among other things, updated the measures implementing the General Regulation and incorporated into national law Directive (EU) 2016/680 of the European Parliament and of 27 April 2016 on the protection of individuals with regard to the processing of personal data.

In this context, the societe anonyme with the name "ADMIE (IPTO) HOLDING SA" and the distinctive title "IPTO HOLDING SA" (hereafter, for the sake of brevity, the "Company"), having the obligation to fully comply with the framework for the protection of personal rights (hereinafter referred to as "Personal Data") and substantial safeguards, in the context of its activity, the confidentiality and security of Personal Data of its employees, shareholders, members of its institutions and services, as well as every third party trader and contractor in general (suppliers of goods and services, etc.), which fall within the meaning of the Subject of personal data, has already adopted and implements a series of policies, procedures and measures, organizational and technical, that integrate into the principles of the General Regulation and the provisions of the overall relevant regulatory framework, regarding the elaboration of Personal Data, their transmission, their maintenance, the policy of consent of the Personal Data subjects, the protection of these rights, as well as the treatment of any violation of Personal Data.

The purpose of this handbook "Privacy Policy and Security of Personal Data" is to record and summarize the principles, policies and protection measures of Personal Data applied by the Company, as the person responsible for processing of Personal Data and / or performing Personal Data processing, during exercise its activity in such a way as to ensure that the relevant rights of the subjects of the Personal Data, as regards the confidentiality and security of their data, are fully respected.

The sub-chapters of this manual "Privacy Policy and Security of Personal Data", which is applied by all the organs and services of the Company and

governs all its activities and operation, describe the basic concepts and principles of the law of protection of Personal Data, the measures that the Company is required to take as a Controller (but also as the executor of the processing), both the organizational and technical security measures, as well as the physical security measures of the Personal Data are recorded and the Company's compliance policies are formulated in (EU and national) Personal Data legal framework.

CHAPTER I

DEFINITIONS - PRINCIPLES GOVERNING IFRS TREATMENT

1. Definitions

Article 4 of the General Regulation defined the content of the terms used in its regulations and which are generally found in the legislative and contractual texts for the protection of the safety of Personal Data. This section sets out the content of the terms defined by this provision and used in this manual, and specifies, where necessary, the specific content that these terms may take on for the purposes of the Personal Data security policy, in within the operation and activity of the Company. It is noted that the conditions, contained in Article 4 of the General Regulation, but are not used in this manual, in particular as they relate to forms of processing that do not take place in the context of the Company's operation or legal relationships not found in its field of activity, are not included in the list below.

- **"Personal Data":** Any information relating to an identified or identifiable natural person ("data subject") · an identifiable natural person whose identity can be ascertained directly or indirectly, in particular by reference to an identity item in name, ID number, position data, online ID or one or more factors that characterize the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

- **"Processing":** Any operation or sequence of operations performed with or without the use of automated means, on personal data or on personal data sets, such as collection, registration, organization, structure, storage, customization or alteration, retrieval, retrieval of information, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, restriction, deletion or destruction.

- **"Restriction of processing":** The labeling of stored personal data in order to limit their processing in the future.

- **"Archiving system":** Any structured set of personal data, which are accessible based on specific criteria, whether this set is centralized or decentralized or distributed on a functional or geographical basis.

- **"Managing Director":** The natural or legal person, public authority, service or other body which, individually or jointly with others, determines the purposes and manner of processing personal data · when its purposes and manner determined by Union law or the law of a Member State, the controller or the specific criteria for his appointment may be laid down by Union law or the law of the Member State.
  For the purposes of this manual, the Managing Director is the "SOCIETE ANONYME IPTO HOLDING S.A." and the distinctive title "ADMIE HOLDING S.A." (now the "Company") based in Athens, Dyrrachiou and Kifisou str. no. 89.

- **"Perform the Processing":** The natural or legal person, public authority, service or other body that processes personal data on behalf of the controller.
  For the purposes of this manual, the Processing is the Company or any other natural or legal person, public authority, service or other entity that processes, in accordance with the General Regulation and the overall Union or national regulatory framework, personal data on behalf of the Company or data transmitted to it for processing, legally or under contract, by the Company.

- **"Recipient":** The natural or legal person, public authority, service or other body to which personal data is disclosed, whether it is a third party or not. However, public authorities which may receive personal data in the context of a specific investigation under Union or Member State law shall not be considered as recipients; such data shall be processed by those public authorities in accordance with applicable data, depending on the purposes of the processing.

- **"Third party"**: means any natural or legal person, public authority, service or body, with the exception of the data subject, the controller, the processor and the persons who, under the direct supervision of the controller or the executor are authorized to process personal data.

- "**Consent of the data subject":** Any indication of will, free, specific, explicit and fully aware, by which the data subject expresses that he agrees, with a statement or with a clear positive action, to process the personal data concerning it.

- **"Violation of personal data":** The breach of security that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed.

- **"Genetic data":** Personal data relating to the genetic characteristics of a natural person inherited or acquired, as obtained in particular from the analysis of a biological sample of that natural person and which provide unique information about his physiology or health that natural person.

- **"Biometric data":** Personal data which result from special technical processing, linked to natural, biological or behavioral characteristics of a natural person and which allow or confirm the unmistakable identification of that natural person, such as facial images or fingerprints.

- **"Health data":** Personal data relating to the physical or mental health of a natural person, including the provision of health care services, which disclose information about his or her state of health.

- **"Supervisory Authority":** An independent public authority established in accordance with Article 51 of the General Regulation. For the purposes of this manual, the supervisory authority is the Personal Data Protection Authority.

2. Principles governing the processing of Personal Data

Article 5 of the General Regulation sets out the principles that should govern the Personal Data security policy and procedures. The Company fully complies with these principles, both by taking specific measures required for their fulfillment, in all cases of Personal Data processing, as well as by the continuous care to ensure the observance of these principles at all levels of its operation and its fields of activity. Particularly:

According to par. 1 of article 5 of the General Regulation, Personal Data:

a) They are subjected to lawful and legitimate processing in a transparent manner in relation to the data subject ("legality, objectivity, transparency").

- ✓ The Company takes all necessary measures to ensure that the processing of Personal Data is always done in accordance with the provisions of the General Regulation and national legislation and always under conditions of objectivity, without entering into the processing of data other than its objective and legal purpose and

transparency, so that the subject of Personal Data is always aware of the purpose, the conditions for processing his data and the measures taken to protect them.

b) Collected for specified, express and lawful purposes and not subjected to further processing in a manner incompatible with those purposes.

- ✓ The Company does not collect and process Personal Data of its employees, shareholders, members of its Board of Directors or third parties, despite the clearly defined framework of its statutory purposes and the legislation governing the organization, operation and operation of public limited companies. In particular, the Company collects and processes Personal Data provided by the employees themselves, at the conclusion of their employment contract or later (exclusively for the purposes of exercising the rights and fulfilling the mutual obligations deriving from the employment relationship, in accordance with the individual contract, the practice of exploitation, the collective regulations and the law in force and governing the employment relationship), its shareholders Company, during the establishment of their shareholder relationship with the Company or thereafter (exclusively for the purposes of fulfilling the mutual rights and obligations arising from the shareholder relationship and the relevant legislation in force), the members of the Company's bodies and services (upon their acquisition of this capacity or thereafter, exclusively in the context of fulfilling their role, in accordance with the Company's Articles of Association and the relevant legislation in force) and third parties or counterparties of the Company (exclusively for the purposes of fulfilling the mutual rights and obligations arising from the transaction / contractual relationship and the law), as well as the Personal Data that legally fall to the Company, in the context of the exercise of its activity and its general operation, in accordance with its Articles of Association and the law. The Company processes this data only for the fulfillment of its statutory purposes and within the framework described by its Statute, its Internal Regulations, its Corporate Governance Code and the current legislation and in particular the legislation on public limited companies, the stock market legislation, market abuse legislation and Law 4389/2016, as applicable.

  The Personal Data are used exclusively for the purposes mentioned herein and are not transmitted to third parties, unless absolutely necessary, for the fulfillment of these purposes and the legal obligations of the Company. In any case, the further transmission of IFRS to third parties requires the explicit consent of the data subjects and the Company undertakes to always seek their consent, unless the transfer is necessary for the Company to fulfill its legal obligation to the Greek

State, the social security institutions, the Hellenic Capital Market Commission or another administrative or judicial authority.

c) They are appropriate, relevant and limited to the extent necessary for the purposes for which they are processed ("data minimization").

- ✓ The Company does not collect or process any Personal Data of its employees, members of its institutions or services or third parties, other than those absolutely necessary for the fulfillment of the above purposes.

d) It is accurate and, where necessary, updated; all reasonable steps are taken for the immediate deletion or correction of IFRS that are inaccurate in relation to the purposes of the processing ("accuracy").

- ✓ The Company always seeks and plans the appropriate measures, so that the Personal Data it collects and processes are accurate and timely, and whenever necessary and after contacting the subjects of the Personal Data, make the necessary corrections and / or deletions of data that are not accurate, in reference to the purposes of the processing.

e) They are kept in a form that allows the identification of data subjects, only for the period required for the purposes of processing Personal Data; Personal Data can be stored for longer periods, as long as they are processed only for archiving purposes in the public interest , for the purposes of scientific or historical research or for statistical purposes, in accordance with Article 89 par.1 of the General Regulation, applying the appropriate technical and organizational measures required by the General Regulation to safeguard the rights and freedoms of the data subject ("restriction of the storage period ")

- ✓ The Company does not maintain Personal Data in a form that allows the identification of data subjects, except for as long as necessary, for the aforementioned legal purposes of processing them. It reserves, however, the right, if this is deemed necessary or requested by a public authority, for reasons of public interest or for the purposes of scientific or historical research or for statistical purposes and within the framework of applicable law, to maintain stored Personal Data of its employees; members of its institutions or services or third parties and for a period to be extended after the expiry of the relevant contractual

ties, taking in each case the necessary and appropriate technical and organizational measures to protect the confidentiality of Personal Data and to fully ensure the relevant rights and freedoms of their subjects ("limitation of the storage period").

f) They are processed in a way that guarantees the appropriate security of the Personal Data, including their protection against unauthorized or illegal processing and accidental loss, destruction or deterioration, using appropriate technical or organizational measures ("integrity and confidentiality").

- ✓ The Company takes all necessary and appropriate organizational and / or technical measures (as specified below), in order to always safeguard the safety of the Personal Data being processed and to prevent any processing by unauthorized persons or their illegal processing or loss or damage.

The Company, as the controller, bears the responsibility and is always able to prove its compliance with the above principles.

CHAPTER II

SECURITY MEASURES

1. Organizational Security Measures

A. Security Officer - Data Protection Officer

The company appoints a Data Security Officer for Personal Data, a natural person, employee or member of its institutions or services or a third party, who provides his services to the Company, in any contractual relationship. The Security Officer for Personal Data is in charge of the ongoing care for the implementation and application of the organizational and technical security measures and the physical security measures of the Personal Data that the Company receives, as they are set out below.
The Company is not obliged to appoint a Data Protection Officer (DPO) according to article 37 par. 1 of the General Regulation (especially in view of the fact that it does not constitute a public authority or body, the

main activities of the Companies do not constitute processing operations which, due to their nature, scope and / or purposes, require regular and systematic monitoring of data subjects on a large scale, and the main activities of the Company do not constitute large-scale processing of special categories of personal data according to article 9 of the General Regulation and data related to criminal convictions and offenses referred to in Article 10 of the General Regulation), however, may, for the most complete and effective possible protection of the security of the Personal Data of its members, voluntarily make the appointment of a Data Protection Officer, according to par. 4 of the same article. In this case, either an employee or a member of the management bodies or the services of the Company can be appointed as the Head of Protection of Personal Data, if he has the necessary qualifications according to the General Regulation and in particular expertise in the field of law and practices for protection of Personal Data and fulfills the necessary guarantees of personal and operational independence against the Controller and / or the Executor, or, following the conclusion of a relevant contract, a third legal / natural person who has the necessary qualifications and guarantees.

The Data Protection Officer, if designated, participates appropriately and in a timely manner in all matters related to the protection of Personal data and receives, from the Company, any necessary assistance in the performance of his duties, as well as the necessary resources and access in processing operations, for the meaningful fulfillment of these tasks. Also, the Data Protection Officer does not receive instructions on how to perform his duties and is not subject to any sanctions because he performed his duties, while he is accountable only to the Board of Directors of the Company.

In case of appointment of a Protection Officer, the employees of the company, the members of the management bodies or the services, the shareholders, third parties whose Personal Data are processed by the Company, can contact the Data Protection Officer, for any issue related to the data processing and by exercising their related rights.

The Data Protection Officer, if designated, is committed to maintaining confidentiality or confidentiality regarding the performance of his duties, which include in particular:

- Continuous information and advice to the Company as the controller and / or to each processor and their employees, regarding their obligations under the General Regulation (GDPR) and the overall regulatory framework for Personal Data protection. In this context, the Head of Personal Data participates

in discussions / meetings within the Company on issues related to the management / processing of Personal Data.

- Monitoring compliance with the General Regulations and current legislation and with the approved safety protection policies of Personal Data, including the delegation of responsibilities, awareness and training of participants in processing operations and related controls.

- Providing advice, when requested, regarding the impact assessment regarding the protection of Personal Data and monitoring its implementation.

- Cooperation with the Personal Data Protection Authority.

- Any action required in the capacity of the Data Protection Officer as a point of contact with the Personal Data Protection Authority, including prior consultation under Article 36 of the General Regulation or any other necessary consultation as appropriate.

- Carrying out the necessary notifications in case of violation of Personal Data.

- The diligence of the issuance of the destruction certificate of the Personal Data.

- The examination of the complaints of the Subjects of the Personal Data.

Unless a Data Protection Officer has been appointed, the above duties are assigned to the Security Officer of Personal Data, who performs them with the assistance of the designated competent bodies, services or employees of the Company.

B. Organization / Management of the personnel, services and management of the Company in matters of protection of Personal Data.

i. Restrictions on the access of the Company's personnel, management bodies and services to Personal Data, depending on their role and in accordance with the necessary measure.

The Company has formed and implements a division of duties and responsibilities of its staff members, administrative bodies and services - in

the context of the responsibilities defined by the Articles of Association, the Internal Rules of Procedure and the law - by organizing the respective procedures, according to in order to identify specific roles in the management of the regular operations and therefore a specific framework for the participation of each executive of the Company in specific aspects of the necessary elaboration of the Personal Data. In particular, each member of the staff, management bodies and services of the Company has the right to access only the absolutely necessary Personal Data, based on the responsibilities and tasks assigned to him and dictated by his role and in accordance with the relevant authorizations given to him.

The authorizations for access to Personal Data must be reviewed and revised, in any case of change in the role and duties of the staff members, management bodies and services of the Company, in order to always limit access to Personal Data, to the absolutely necessary extent.

The members of the Company, the management bodies and the services of the Company who are authorized to access the absolutely necessary Personal Data processing, must be selected based on the degree to which they guarantee, in terms of technical knowledge and personal / operational independence, the observance of confidentiality and the protection of the safety of Personal Data.

In any case, the Company is obliged to bind the members of its staff, management bodies and services or third parties, who perform Personal Data processing operations on its behalf, with clauses of confidentiality and compliance with the applicable regulatory framework for the protection of privacy and the safety of Personal Data, which should be included, where appropriate, in employment contracts or outsourcing operations or in the contracts of independent services or project assignment, which will connect the Company with the persons that participate, on its behalf, in Personal Data processing operations. The validity of these confidentiality clauses should be extended after the expiration of the relevant contracts (or decisions assigning specific tasks to the members of the company's management bodies, related to the processing of Personal Data) and cover a period of at least 5 years thereafter.

ii. Personal Data security measures after the termination of the contractual relationship or status of the participants in the processing.

After the termination or termination of the contractual relationship of the Company's staff members or after the termination of the membership of the Company's management bodies or services participating in Personal Data processing operations or after the termination or termination of the Company's contractual relationship with third parties acting Personal Data processing operations on behalf of the Company, the latter is obliged to take all necessary measures to ensure the confidentiality and the general protection of the security of the Personal Data, which were observed by the

employee or the member of the management bodies or the services of the Company or by the third party or to which they were entitled access and / or processing. The following measures are indicative (and not restrictive):

- Removal of all Personal Data accounts, credentials and passwords.

- Abolition of the e-mail accounts of the member of the staff or of the management bodies or services of the Company who has ceased to have the right of access and / or processing, due to the termination of his contractual relationship with the Company or his relevant capacity. In case of replacement by another employee or member of the management bodies or services of the Company, the e-mails that may be received by the departed employee or the departed member of the management or services of the Company, will be redirected to the email address of the replacement.

- Obligation to return any material equipment provided to the outgoing employee or to the outgoing member of the Company's management or services, who provides access to Personal Data (including computers or removable media, keys, electronic input cards / login cards).

C. Management of information goods.

i. Physical and electronic file management.

Physical records containing Personal Data (of any type or category) are kept in key locked storage areas, which should be kept by the Company staff member or management body or services authorized to access such records. A second key to access these files will be kept by the Data Security Officer (or - if any - by the Data Protection Officer). In order to protect data security, a copy of the stored physical files will also be kept in electronic form.

Electronic files containing Personal Data (of any type or category) are stored on the Company's servers. These files are accessible only to members of the staff or management bodies or services of the Company, who are specially authorized for this purpose. These files are always accessed using security codes (username and password), unique to each person authorized to access the files.

ii. Data handling outside the Company's premises.

In the event that Personal Data storage material (electronic or physical) is transferred outside the Company's premises, this transfer action is recorded (date and time of departure, persons authorized to use the transferred storage

media, person carrying out the transfer, date and return time, person making the return). Any such transfer is subject to the approval of either the legal representative of the Company or the Data Security Officer (or - if any - the Data Protection Officer).

D. Performing the Processing.

i. Register

The Company is obliged to keep a list of all processors, who handle Personal Data on its behalf, inside or outside its facilities.

ii. Written assignment - General obligations of the Executor of the Processing.

In case the Company entrusts the processing of Personal Data to the Executor of the Processing, the relevant assignment is made in writing and provides that the Executor performs the Processing only by order of the Company, within this and in accordance with the provisions of article 28 of the General Regulation and the relevant legislation in force at the time.

The written contracts must contain, at a minimum, a description of the Personal Data to be processed, the purpose, the place, the manner (procedure), the purpose and duration of the processing, the level of security of confidentiality and the quality of the process processing of the Personal Data, as well as in general the obligations of the Executor of the Processing, which should not fall short of those provided for in Article 28 of the General Regulation.

In particular, in each case, the Executor of the Processing:

- Processes the Personal Data only within the framework of the assignment contract and based on recorded orders of the Company.

- Ensures that the persons authorized to process personal data have committed to confidentiality or are under the appropriate regulatory obligation of confidentiality.

- Takes and observes all the necessary, as appropriate, organizational and technical security measures provided herein.

- Does not hire another Executor of the Processing, without prior special or general written permission of the Company. In case of general written permission, the Processing Executor informs the Company of any intended changes concerning the addition or replacement of the other processors, thus enabling the Company to oppose these changes.

In any case of a special or general authorization to assign Personal Data processing to another Executor, the contract ensures that all the obligations of the Processing Executor and any organizational and technical security measures provided herein are complied with by the other Executor. Otherwise, the original Executor of the Processing remains fully responsible to the Company.

- Takes into account the nature of the processing and assists the Company with the appropriate technical and organizational measures, to the extent possible, for the fulfillment of its obligation as a Processing Manager, in requests for the exercise of the rights of Personal Data Subjects.

- Assists the Company in ensuring compliance with its obligations as a Responsible Processor, taking into account the nature of the processing and the information available to it.

- At the Company's discretion, deletes or returns to the Company all the Personal Data that have been processed, after the end of the provision of processing services and deletes the existing copies, unless the law requires their storage.

- Makes available to the Company all the necessary information to prove compliance with its obligations, allows and facilitates any relevant audit, including inspections carried out by the Company or another person authorized by it.

The Company must, in any case, ensure the observance, by the Executor of the Processing, of its obligations and in general of the terms of the present, the General Regulation and the current legislation.

iii. Security measures concerning the Executors of the Processing.

In addition to its obligation to comply with the organizational and technical security measures of Personal Data provided for herein, the Processing Officer (a) grants access rights to members of its staff only when necessary for the performance of its contractual obligations, granting the minimum required authorizations, which are abolished at the end of the contract, b) exhausts, in any case where maintenance or upgrade of equipment bearing Personal Data, any possibility of carrying out these works within the Company, while, when this is not possible, always ensures that the relevant work is performed at a level of security at least appropriate with what is defined herein, c) ensures that each of its employees participating in the processing of Personal Data is bound in writing by an appropriate confidentiality agreement, which ensures a level of protection at least equivalent to that of the respective contracts of members of the staff or management bodies or services of the Company.

E. Destruction of data and storage media.

In any case of destruction of physical or electronic files containing Personal Data, appropriate measures shall be taken to ensure the complete and permanent deletion of such data, in order to exclude their further illegal and improper processing, in particular any form of their disposal to third parties.

In this context, in particular and at least full compliance with Directive 1/2005 of the Data Protection Authority, for the safe destruction of Data Personal, after the end of the period required to achieve the purpose of the processing, must be fully complied with. A safe way of destroying Personal Data is considered to be any set of material actions, procedures and measures, after the implementation of which, it becomes impossible to identify the subjects of Personal Data, in an irreversible way, which makes it impossible to recover, after their destruction, Personal Data with technical or other means.

The Data Security Officer (or - if any - the Data Protection Officer) ensures the implementation of appropriate control mechanisms for the proper observance of the destruction process applied by the Company.

The audit should be assigned to authorized, for this purpose, members of the Company's staff.

In the event that the destruction of Personal Data is carried out, on behalf of the Company, by a person who does not belong to the members of the staff or the management bodies or the services of the Company (ie by the Executor), the Company is obliged to make the relevant assignment only in writing. This written assignment must indicate the measures to be taken by the Executor of the Processing, for the safe transport of the Personal Data to the site of destruction (if the destruction cannot take place at the Company's premises), any intermediate storage locations of the Personal Data, the manner of destruction, as well as the maximum time allowed, from the moment of delivery of the data by the Company to the Executor, until their final destruction. In addition, any additional instructions of the Company regarding technical and organizational destruction measures should be mentioned, as well as the exact details of any third parties (subcontractors) who are going to carry out part or all of the destruction of the Personal Data on behalf of the Processing Executor. Furthermore, it must be ensured in any case that the Company has the power to dispose and control the data, until their final destruction. Therefore, the Processing Executor must keep separately the Personal Data to be destroyed of the Company, with which he concludes the relevant contract. The Executor must be able to apply the appropriate technical and organizational measures for the safe destruction of Personal Data and have provided a corresponding process of destruction and disaster control with that of the Company. The natural persons added by the Executor of the Processing must be specifically obliged to ensure the confidentiality of the processing.

The Company, indicatively and not exclusively, applies the following Personal Data destruction measures:

- Shredding of documents into strips, using special document shredding machines, within the Company's premises and by authorized members of the staff or its management bodies or services.
- Mash / recycle documents.
- Incineration of the data substrate material.

After the disaster, an IFRS Destruction Protocol is drawn up, which contains at least the following information:

- Date of destruction of Personal Data,
- Description of the destroyed IFRS,
- Method of destruction,
- Name of the responsible member of the staff or of the management bodies or services of the Company who is responsible for the destruction or (in case the destruction has been assigned to the Executor) of the Executor of the Treatment (in the latter case, the contract is also mentioned to the Executor).

For the safe destruction of Personal Data in electronic form, simply deleting them (e.g., with the command "DELETE") is not enough, as, in this way, only the reference to the data is deleted, while the IFRS themselves may be recoverable using special software programs. As a result, IFRCs stored on rewritable media (e.g., hard disk, rewritable DVD or CD) are corrupted by overwrite them. Destruction can also be done using special programs (file-erasers, file-shredders, file-pulveritizers). In everyday cases data destruction, an alternative way of destruction may be to format the substrate material.

In the case of planned destruction of the data set, an alternative way of destruction (for particularly critical data) is the physical destruction of the substrate material itself (e.g., by crushing, pulverization, incineration), subject to special provisions regarding with environmentally friendly waste specific management.

The destruction of data includes the destruction of all backups (back up) maintained by the Company, if this is practically and technically feasible.

Scheduled data destruction must be accompanied by a Data Destruction Protocol, in accordance with the above.

The Data Security Officer (or - if any - the Data Protection Officer) takes care of the training of the members of the staff or the management bodies or the services of the Company in the process and the methods of destruction of the Personal Data.

F. Training of members of the staff, management bodies and services of the Company.

The Company continuously and effectively seeks the training of its staff members, management bodies and services in matters of Personal Data protection, compliance with the applicable regulatory framework and compliance with the organizational and technical measures described herein (such as in particular the use of non- predictable passwords and passwords, how to detect, record and report security breaches, the proper use of e-mails and removable storage media, the process of destroying Personal Data, etc.).

The training, when hiring or assigning tasks related to the processing of Personal Data, should include at least the notification of this Personal Data privacy and security manual adopted by the Company, as well as information on the Personal Data violation management procedures. Training should be ongoing and always monitor significant changes in security procedures or the emergence of significant security issues.

The training is done by the Data Security Officer (or - if any - the Personal Data).

G. Control.

The Data Security Officer (in collaboration with the Personal Data, if any) must conduct, at least once per calendar year, a sample compliance check of the Company and its staff members, management bodies and services involved in the processing of the IP, in the current privacy and security policy of Personal Data, with the aim of reviewing its proper implementation and assessing the effectiveness of organizational and technical security measures.

Any findings of the audit are recorded and submitted in writing to the Board of Directors of the Company, together with the written relevant suggestions of those who conducted the audit, regarding the appropriate corrective - additional measures that the Company should take.

H. Personal Data treatment impact assessment.

In cases where specific forms of processing (particularly the use of new technologies), taking into account their nature, scope, context and objectives, may pose a high risk to the relevant rights and freedoms of Personal Data, referred to in Article 35 of the General Regulation (and in the relevant Guidelines), as well as in no. G / EX / 8187 / 16-10-2018 relevant Catalog issued by the Data Protection Authority, pursuant to par. 5 of the said article, the Company carry out an impact assessment of the specific forms of Personal Data processing.

I. Overview - evaluation - review of the level of effective protection.

This Privacy and Security Manual, as well as the measures and procedures set out in it, are regularly reviewed in order to continuously and effectively assess the level of security provided and to assess the degree of compliance with developments, updates and redesigns of the relevant EU and national regulatory framework.

In any case, the review of the Company's policy is required in particular in cases of substantial changes, a) in the organizational structure and the staff of the Company, b) information systems, c) security requirements, d) technological developments and e) forms, methods and processes of Personal Data processing.

This may also be revised in cases where, following internal or external audits or the recording of cases of Personal Data violations, the inadequacy or ineffectiveness of the data security measures provided for therein is established.

The Security Officer (in collaboration with the Data Protection Officer, if any), is responsible for suggesting the need for updates / revisions to this policy, as well as the measures and procedures described in it, which will take effect upon written their approval by the management of the Company.

2. Technical safety measures.

A. Access control.

i. User account management.

The Company formulates and adheres to specific specifications for managing the accounts of the users of its files, which include specific procedures for

adding / changing properties and deleting accounts. Each user of the Company's files accesses with a different account. In particular, with the hiring of each employee or with the assignment of specific roles to a member of the management bodies or services of the Company that presuppose or imply access to electronic files of Personal Data, his data is registered in the "active directory" of the Company, with a specific name user and specific password.

ii. Access control mechanisms.

The Company organizes and implements mechanisms that do not allow access to resources / applications / files that contain Personal Data to unauthorized users and ensure the guaranteed correct identification of users, while ensuring, at a technical level, the specific and fully limited assignment of access rights / authorization to each user.

In particular, the Company has two different levels of electronic "firewall":

The first level ensures the rules for the proper operation of the Company's network, while protecting the Company from outside threats.

The second level is protection against malicious e-mails, which come from either external or internal agents, who may have been infected with a virus.

iii. Password management.

The Company has a specific policy for the management of users' passwords, which includes uniform acceptance rules regarding the minimum length and permissible characters of passwords (password complexity), the historicity of the password and the frequency of its change. All user passwords / passwords must meet at least the following criteria:

- Contains at least 8 alphanumeric characters,
- Contain lowercase and uppercase letters,
- Contain at least one numeric digit,
- They contain at least one special character / symbol (e.g., $, %, -, {}. [,], ¡,?, =;).

Unacceptable passwords are in particular those that have the following characteristics:

- Contains less than 8 characters,

- Consist exclusively of words that can be found in a dictionary, including foreign languages or dialects or slang, etc.

- Contain personal information, such as dates of birth, addresses, telephone numbers, names of family members or pets, known characters / heroes, etc.,

- Contain information related to the work, such as building addresses, system commands, Company initials or marks, hardware / software companies, etc.

- Contain repeating patterns or sequences of numbers (such as aaabbbccc, 12345, 54321, etc.),
-

The passwords should not be recorded anywhere (in a physical or electronic file, mobile phone, tablet or anywhere else), nor should they be disclosed to third parties, inside or outside the Company or communicated by e-mail, telephone or other means. Instead, they should be considered by their users as sensitive confidential information. For this reason, passwords that can be easily saved by the user should be selected. If passwords are kept electronically as part of the user authentication process, then it must be in an illegible form, from which it must not be possible to recover their original form. Users are also required to change the (default) password provided to them from the beginning, as well as to change their password at regular intervals (less than 4 months).

If possible, each user should have a different password for each application of the Company, access to which requires the use of a password.

iv. Unsuccessful access attempts.

In the event that any user enters the wrong password three times in a row, the Company may reconsider its authorization to access that file.

v. Inactivated computer.

In order to avoid cases of unauthorized third-party access to Personal Data, due to an open, unsupervised computer, the Company has provided the possibility of automatic disconnection of the computer (after three minutes of inactivity) and / or activation of the computer screensaver, for reactivation which will require the use of a password.

B. Backups.

The Company receives backup copies of the original computer data held by members of its staff or organs or services and containing Personal Data (documents, photographs, and electronic storage media with Persona Data). The copies are received on a daily basis and, after the date of their receipt is marked, they are stored weekly in a storage area outside the Company's headquarters, which locks and the key is kept by the Data Security Officer.

Every month, the Data Security Officer checks the integrity / reliability of the copies received, in order to ensure the correct recovery of the Personal Data from the backups, in case of emergencies and loss or destruction of the Personal Data for another reason. (e.g., hardware failure).

C. Computer configuration.

i. Malware protection.

The Company has malware protection systems on all computers (both the personal computers of members of the staff or of the Company or the services that provide access to Personal Data and the servers -servers-) where they are maintained and subject to Personal Data processing, using antibiotics (antivirus) as well as firewalls. In these programs, the appropriate security updates are installed at regular intervals.

In case of malfunction of antibiotic programs or firewall programs, informational messages appear on the computer screen. Such messages must be reported directly to the Data Security Officer.

Files attached to e-mails whose sender is unknown or files of unknown type should not be opened. In this case, the Data Security Officer should be informed immediately.

If there is even a suspicion that the computer has been infected by malware, it should be turned off immediately and the Data Security Officer should be informed.

The members of the staff, organs and services of the Company are regularly informed about the proper use of computers and the internet, but also about the appropriate actions to deal with malware.

ii. Computer settings.

Ordinary user actions (authorized or not) on computers, which affect their overall configuration (e.g., disabling antibiotic programs, installing new programs or changing security settings, etc.) are prohibited. The Data Security Officer conducts periodic inspections of the installed software of the

Company's computers, to identify any programs installed other than those approved.

In case the installation of specific software is required, in order to perform a task, the interested user should submit a relevant request in writing to the Data Security Officer, in which he will state the software he is interested in installing on his computer and will adequately justify the reasons which make its installation necessary. Once the request is accepted, the software is installed on the computer either by or in the presence of the Data Security Officer.

ii. Computers - servers.

If a computer is used as a server for other computers, then it will not be used as a workstation for a user.

iv. Computers with internet access.

Personal Data may not be stored on computers connected to the Internet (unless this is necessary due to insufficient technical resources of the Company or if necessary due to the role / responsibilities assigned to the computer user).

D. Logs of user actions and security events.

i. Keeping and checking logs.

In systems with any special security requirements, logs of all users' logfiles are kept, including the actions of the system administrators, as well as the security events. These files will be protected with a password known only to the Data Security Officer.

These files may be accessed by the Data Security Officer (or the Personal Data - if any), the system administrators and any other members of the Company's staff or institutions or services in charge of responsibilities for managing security incidents, upon written authorization.

Access to these files is recorded and the relevant logs are kept by the Data Security Officer.

ii. Special actions to be recorded.

The action logs must at least keep the following: The ID of the user who requested the access to the Personal Data, the date and time of the relevant request, the system through which the access was requested (computer, software program, etc.), as well as if the files were finally accessed. Also

requested are requests to print files with Personal Data, as well as changes to critical system files or user rights. Furthermore, logs of unauthorized access attempts and changes in the configuration of applications and systems, the predetermination of critical events (events) are kept. These logs are supervised by the Data Security Officer, who generally addresses any indication that may indicate an attack, such as port scanning efforts.

iii. Delete logs.

It is not possible to delete system logs by a single person. Such deletion should be done in the presence of at least two people, among whom should be at least the Data Security Officer.

E. Communication security.

i. Network device testing.

The Data Security Officer is in charge of controlling the devices connected to the network (in terms of access to them, but also their use).

ii. Remote access.

Remote access to systems (e.g., from maintenance companies or from members of the staff or the organs or services of the Company) is made through secure channels with the possibility of identification and encryption. Please note that remote access technologies (e.g., Remote desktop, Ammy, wireless, etc.) are only allowed to authorized persons for whom they are absolutely necessary, within the scope of their responsibilities. Remote access is done under the supervision and control of the Data Security Officer and is recorded.

iii. Communication channel.

Communication between computers / nodes is done through a sufficiently secure communication channel (e.g., using encryption and / or private lines with controlled physical access).

iv. Network protocols.

It is forbidden to use security-sensitive protocols, such as FTP telnet (where no encryption is done) and, when services of such protocols are needed, use corresponding secure ones (such as SFTP, SSH).

F. Software Security

i. Application design

The basic principles of Personal Data and privacy by design are already taken into account when designing applications used for the processing of personal data.

Applications must follow the principle of data minimization as well as data quality and include the ability to delete data after the time required to accomplish the purpose of the processing.

They must also enable the proper operation of all the necessary technical safety mechanisms to protect the Personal Data from accidental or unlawful destruction, accidental loss, deterioration, prohibited dissemination or access and any other form of improper processing.

ii. Application development

In case of application development either internally by the Company or by an external partner, a secure software implementation process should be provided, in order to identify any security vulnerabilities before it enters an operational phase.

Especially in the case where the development of applications is done by an external partner, there should be security specifications of the application in the software requirements description document, which will be included in the contract with the partner.

iii. Operating system file protection

System files, system test data, and source codes of software programs must be controlled and protected from unauthorized access or modification.

G. Change management

i. Change management policy

In the context of the policy of change management in the Company's information systems, the Data Security Officer records all requests for changes, determines the persons who have the right to approve the changes, the criteria by which it is determined whether the proposed changes are in accordance with the policy of Personal Data protection and confidentiality, as well as the timetable for implementing the changes.

No changes will be made unless required to perform the user's tasks properly.

ii. Test environment

Before launching software updates, they should be tested, at the individual application level and at the operating system level, in a test environment.

Software development takes place in a test environment, which is isolated from the production system and updated. When developing or upgrading software and testing it, trial data is used rather than actual production system data, unless absolutely necessary and there is no alternative.

If necessary, real data may be used in anonymous form or, alternatively, the test should be limited to data that are strictly necessary for the purposes of the test.

3. Physical security measures

A. Physical access control

i. Physical access to data storage facilities and information systems.

In the area where the physical equipment (including telecommunication and network cabling) is maintained Personal Data and information systems support, access is only allowed to authorized personnel (and, if technically possible, using a security code). Access to the specific natural areas is recorded.

ii. Keeping a list

The Data Security Officer maintains an up-to-date list of the physical access rights of the members of the staff, the management bodies and the services of the Company who have codes or entrance cards or keys in places critical to security. These lists are subjected to regular review.

B. Environmental safety - Protection against natural disasters

The Company is obliged to take all necessary measures to protect the facilities, critical areas, information devices and systems, offices and the physical record keeping area, from damages that can be caused by natural disasters or malicious actions, such as floods, overheating, fire, earthquake, explosion, water leakage, power outage, burglary / theft, vandalism, etc. Indicative measures taken in this direction are: Alarm, security doors and windows, fire protection, removal of equipment from water pipes and dust sources, uninterruptible power supply through stabilizers / generators, etc.

C. Report of documents

i. Placing folders

Folders containing Personal Data (physical file) must be placed in lockable enclosures and not exposed to public view.

ii. Transfer of folders

Each transfer of the physical file or its data to different offices or facilities of the Company, is recorded by the employee or the member of the organs or services of the Company, who is responsible for their maintenance.

iii. Clean desk policy

They should not be left exposed on unsupervised offices, documents and portable storage media containing Personal Data or any kind of confidential information.

The members of the staff, organs and services of the Company should ensure that all personal data/ confidential information (in printed or electronic form) is safe in their workplace, both at the end of working hours and in the absence from their place of employment.

Computers should be locked (screensaver) when the user is away from work and turned off at the end of working hours.

Drawers and enclosures containing personal data / confidential information should be kept locked and locked when unattended.

Keys used to access premises where personal data / confidential information is stored should not be left exposed on desks.

Laptops should be locked in a drawer or closet at the end of business hours.

Passwords should not be written on notes attached to the computer or exposed in any way to public view.

Prints containing personal data / confidential information should, after use, be cut into strips, in a document shredder.

Personal data or any confidential information on a whiteboard should be deleted immediately after use.

Laptops containing personal data / confidential information should be kept in locked areas, even when away from the workplace (e.g., at the user's home).

Portable mass media (such as CDROM, DVD, and USB) should be stored in a lockable area.

Any document containing personal data/ confidential information should be taken away immediately by photocopiers, printers, fax machines, in order to ensure in any case that they are not left exposed to persons not authorized to use them.

CHAPTER III

CONFORMITY POLICIES TOWARDS GENERAL REGULATION AND CURRENT LAW ON PROTECTION IFRS

A. PERSONAL DATA TRANSMISSION POLICY

The General Regulation sets out specific conditions for the transmission of Personal Data to countries or international organizations outside the EU. After taking into account all available information on the recipient of the Personal Data to be transmitted, any necessary terms and conditions for the transmission are identified.

In any case, the terms and conditions of data transmission outside the EU differ depending on whether the transmission takes place in countries or international organizations where, according to a relevant Commission decision, an adequate level of personal data protection is provided and in countries where the level of protection is insufficient. Particularly:

With regard to the transmission of personal data to countries / international organizations, for which no relevant decision has been issued on an adequate level of protection, pursuant to Article 25 par.6 of Directive 95/46 / EC, must, in any case, a minimum set of protection guarantees is ensured through:

- a legally binding and enforceable instrument, between public authorities or bodies,

- binding company rules, in accordance with Article 47 of the General Regulation,

- standard personal data protection clauses, issued by the Commission, in accordance with Rule 93 par.2 of the General Regulation,

- standard personal data protection clauses, issued by the Personal Data Protection Authority and approved by the Commission, in accordance with Article 93 par. 2 of the General Regulation,

- an approved code of conduct, in accordance with Article 40, together with binding and enforceable obligations of the Controller or Processor in the third country, to apply the appropriate safeguards, including the rights of personal data subjects,

- an approved standardization mechanism, in accordance with Article 42 of the General Regulation, together with binding and enforceable obligations of the Controller or Processor in the third country, to apply the appropriate guarantees, including the rights of personal data subjects,

Without prejudice to the permission of the Personal Data Protection Authority, the above appropriate guarantees are provided in particular through,

- Contractual clauses, between the Controller or the Executor and the Controller or Executor or the recipient of the personal data in the third country / international organization. The standard clauses of the EU should be annexed to the relevant contract.

- Provisions for inclusion in administrative arrangements between public authorities or bodies, which include enforceable and substantive rights of personal data.

No special authorization is required for the transfer to countries / international organizations with which there is a relevant decision on an adequate level of protection, based on article 25 par. 6 of Directive 95/46 / EC.

In cases where there is no decision on an adequate level of protection and where the above guarantees are not provided, a personal data transfer cannot take place in principle.

Exceptionally, the above transmission is possible, provided that the following conditions apply:

- The Subject of the Personal Data has explicitly consented to the transmission, having been informed of the potential risks of such a transmission for itself, due to the absence of a decision on an adequate level of protection and appropriate guarantees.

- The transmission is necessary for the execution of a contract between the Subject of Personal Data and the Company or for the

implementation of pre-contractual measures taken at the request of the Subject.

- The transmission is necessary for the establishment, exercise or support of legal claims.

- The transmission is necessary to protect the vital interests of the personal data Subject or other persons when the personal data Subject is physically or legally unable to give consent.

B. PERSONAL DATA CONSERVATION POLICY

An absolutely necessary condition for ensuring an adequate and effective level of protection of personal data is to ensure that they are always subject to proper management / processing, throughout their life cycle, i.e. from their collection to their final and final destruction. . Proper planning of the destruction of personal data is at the same time a regulatory requirement for their effective protection, but also an essential condition for their legal processing.

This manual defines the principles of maintenance and destruction of IFRS collected and processed by the Company, in order for the relevant policies applied to be in full compliance with the General Regulation and applicable personal data protection legislation.

The personal data maintenance policy, which ensures in any case that **personal data are maintained for a period not exceeding what is absolutely necessary to meet the purposes of the processing**, is a central component of the framework of personal data. Furthermore, more specific regulatory provisions, which derive directly from the law or related contractual commitments, set out the minimum retention period of personal data before they can be destroyed, as well as the conditions under which personal data must be destroyed, even before expiration of their minimum retention period.

This policy applies **to any personal data processing that the Company performs as the Controller or as the Processor**.

1. Periods of conservation / destruction.

For the purposes of determining the retention policy of personal data and determining the time of their destruction, their treatment is determined based on the importance of their preservation, in relation to the time required to fulfill

the purpose of their processing and the actual / legal possibilities of their destruction. , as follows:

Period of Use	Personal data are still necessary to meet the purposes of processing.
Exclusion Period	Personal data are no longer necessary to meet the purposes of the processing, however they still need to be retained for a period of time to meet legal or accounting purposes. During this period, the personal data ▪ They cannot be destroyed, ▪ They are only available to a limited number of persons, i.e. only to those who are responsible for fulfilling the legal or accounting maintenance purposes.
Disaster Period	Personal data are no longer required for processing purposes or other legal / accounting purposes. Therefore, personal data must be destroyed (deleted or anonymized) in accordance with personal data protection legislation.

2. Principles of Conservation and Destruction.

A central guiding principle of personal data conservation policy is the condition that, when personal data **are no longer necessary** for processing purposes and **there is a possibility** (or legal obligation**) to destroy them**, their deletion (or anonymity) becomes necessary.

The formulation of the relevant policy ensures that the records are kept only for as long as necessary and that, when there is no longer a legal reason for their preservation, the relevant records are destroyed in a systematic, controlled and secure manner. For the implementation of the conservation / destruction policy, the following are taken into account:

Minimum Retention Period

The time at which personal data must be maintained. During this period the personal data cannot be destroyed. Usually, this period coincides with the longest interval between:

• The minimum required retention period for legal / accounting reasons and

• The minimum required retention period for the purposes of processing the personal data by the Company.

Maximum Retention Period

The maximum time limit by which personal data can be maintained before being destroyed. This interval is determined by:

- The regulatory framework for the protection of personal data (General Regulation - national legislation), which requires non-maintenance of personal data for longer than necessary for processing purposes (or for other

legal or accounting reasons),
- Any recommendations from supervisory authorities,
- Agreement with the personal data Subject.

Activation event

The event that determines the starting point of the retention period of personal data (e.g. last processing date, contract expiration date, etc.).

In any case, for the more specific determination of both the maximum and the minimum retention period of personal data, the following must be taken into account: a) the provisions of the General Regulation and the national legislation on personal data protection, labor and insurance legislation, tax legislation, legislation on public limited companies, stock exchange legislation, the applicable regulatory framework governing the operation and activity of the Company, b) any special requirements of the Personal Data Protection Authority and c) any special contractual obligations.

3. Special cases of personal data, concerning the internal operation of the Company.

Employees' personal data of the Company: The personal data of the employees will be maintained throughout the employment relationship with the Company and for five (5) years after the termination or in any way the expiration of the term of the employment contract, unless a legal dispute is pending. Subject to personal data with the Company, in which case they will be retained until an irrevocable court decision is issued. From the time of termination or in any way the termination of the employment relationship with the employee until the completion of five (5) years, the personal data will be kept anonymous.

Personal data of any prospective employees are deleted immediately after their job application is rejected.

Personal data for members of the Company's management: They will be retained for as long as the members retain their capacity and for an additional ten (10) years. Especially for the executive members of the Board and the Chief Executive Officer, the personal data will be retained, for as long as they retain their status and for an additional twenty (20) years. From the expiration time of their status above and until the completion of the above defined additional period, the personal data will be kept anonymous.

Personal data of suppliers or third party counterparties: They will be kept for as long as necessary to complete the processing purpose and until the completion of 10 years. From the time of completion of the purpose of processing the personal data until the completion of 10 years, the personal data will be kept anonymous.

4. Application of deletion mechanisms.

For the destruction / deletion of personal data, the destruction mechanisms (automated / manual) provided in Chapter II.1.E hereof ("Destruction of data and storage media") must be applied.

Also, a "Register of Corrupted Files" is created and maintained, where every act of destruction / deletion is recorded.

The requirements of this personal data conservation / destruction policy are taken into account during the design phase of each new system or process under which personal data is processed to enable the personal data to be automatically deleted.

5. Review of personal data maintenance policy - Ensure effective implementation.

This personal data maintenance policy should always monitor developments and changes in the Union and national regulatory framework for the protection of personal data, any recommendations of the Protection Authority of personal data, as well as any changes in the Company's internal organization and operation, in order to keep up to date and, if necessary, be reviewed on a regular basis.

To this end, as well as to ensure the full and effective implementation of this policy, regular checks are carried out on the level of compliance with it and the degree of effectiveness of the relevant measures and policies.

C. CONSENT POLICY

1. Consent as a condition of legality of personal data processing

In any case of processing of personal by the Company, acting either as the Controller or as the Executor of the Processing, it is examined whether the processing is carried out with the consent of the Subject of the personal data or by other legal basis, according to the following.

Any processing of personal data without the consent of the Subject of personal data is prohibited, unless one or more of the conditions of Article 6 of the General Regulation are met and specifically if:

- ✓ processing is necessary for the performance of a contract to which the personal data are a party or to take action at the request of the personal data subject prior to the conclusion of the contract,

- ✓ The processing is necessary for the compliance with the legal obligation of the Company,

- ✓ The processing is necessary to safeguard the vital interest of the personal data Subject or other natural person,

- ✓ Elaboration is necessary for the performance of a duty performed in the public interest, in accordance with national or Union law,

- ✓ The processing is necessary for the purposes of the legal interests pursued by the Company, within the framework of its Articles of Association and the relevant legislation, unless in this case the interest or the fundamental rights and freedoms of the Subject of the personal data that impose the protection of personal data, especially if the Subject of personal data is a child.

2. Processing of personal data of special categories.

The normal course of business of the Company does not presuppose or imply the elaboration of personal data that fall into the special categories provided for in Article 9 of the General Regulation (data, that is, that reveal racial or ethnic origin, political views, religious or philosophical beliefs or trade union affiliation, as well as the processing of genetic data, biometric data for the purpose of sexual orientation).

In any case, the Company fully complies with the provisions of paragraph 2 of the above article, according to which, the processing of personal data belonging to the above special categories, is allowed **only under certain conditions**, such as when the subject of **explicitly consent** to the processing of such personal data for one or more specific purposes (unless Union law or

national law provides that the prohibition may not be lifted by the data subject), **when the processing is necessary for the execution of the obligations and the exercise of specific rights of the Company as the responsible processor or the subject of the data in the field of labor law and the law of social security and social protection** (if permitted by the law of the Union or by the national law or by collective agreement in accordance with national law by providing appropriate guarantees for the fundamental rights and interests of the data subject), when the processing is **necessary to protect the vital interests of the data subject or other natural person, if the data subject is physically or legally incapable of consent**, when the processing involves personal data explicitly disclosed by the data subject , when the processing is necessary for the establishment, exercise or support of legal claims, when the processing is necessary for reasons of substantial public interest, under Union law or national law, which is proportionate to the objective pursued, respects the substance of the data protection right and provides for appropriate and specific measures to safeguard the fundamental rights and interests of the data subject, **or where the treatment is necessary for the purposes of preventive or occupational medicine, assessment of the employee's ability to work.**

3. Necessary characteristics of consent

In order for the provision of the Subject of personal data consent to be a sufficient legal basis for the processing of its data, in each case the characteristics attributed to the concept must be met, according to the definition of Article 4 par. 11 of the General Regulation, as explained and specialized, in accordance with Regulation 2016/679 "Guidelines for Consensus", adopted on 28 November 2017. In particular:

Element of the Definition (Article 4 par. 11 GC)	**Specialization (Guidelines of Regulation2016/679**
"Free"	The Subject of personal data is provided with real, ongoing selection and control over how its data is used. Consent is not considered to have been given freely when

- consent is a non-negotiable part of the terms and conditions for the transaction with the Company and
- The Data Subject is not able to refuse or withdraw its consent without harm.

"Specific"	Consent is given specifically in relation to one or more specific purposes of processing If the Company processes data on the basis of consent and wishes to process the data for a new purpose, it must seek new consent from the Subject of personal data, regarding this new processing purpose. The initial consent does not legitimize further processing purposes.
"Explicit"	The request for consent must clearly state the identity of the Controller (indicate, that is, specifically the Company as Responsible), the type of IFRS that will be processed, the possibility of revoking the consent and the purpose of processing. The provision of necessary information to the Subjects of the IFRS, before the provision of their consent, is necessary in order for them to be able to make informed decisions, to understand the exact object of their consent and to exercise their relevant rights (e.g. revocation of consent).

"Fully aware"	The request for consent must be clear, separate from other terms and conditions, as short as possible, in clear and comprehensible language. Consent can also be obtained through a written or -confirmed- oral statement or by a statement made through electronic means.
"Given with clear and positive energy"	Consent must be obvious and require positive selection action. Consent may also be given by affidavit, although in any case reference must be made to the IT available to the Subject prior to consent.
"Constitutes a manifestation of his agreement"	In cases where there are serious risks, consent is not enough to manifest itself with a simple positive action, but must be provided explicitly on a specific written statement.

As the Subject's consent may be revoked without notice and at any time, consent must not be a condition for the Company to receive a service from the Subject, unless this is the only legal basis for the processing of personal data (if, i.e., does not meet any of the other conditions mentioned above, under C.1) or if it is a case of automated decision making or concerns personal data (and) children under 16 years of age or data transmission outside the EU / EEA.

In cases where it is necessary to obtain the consent of the Subject of personal data, **the Company must collect and keep evidence of the consent.**

4. Duration of consent.

In the absence of a more specific determination, by the General Regulation or the national legislation, of the duration of the consent provided, as such is considered the time during which the consent retains its necessary characteristics (according to the above, under 3). If the purpose or type of processing changes substantially, then the original consent no longer constitutes a sufficient legal basis for processing and a new one should be given. In any case, the consent should be renewed regularly in

order to ensure that the Subject of the personal data remains sufficiently informed of the manner in which its data are used and the way in which its related rights are exercised.

5. Procedure for obtaining consent.

Prior to obtaining the consent, all the necessary information is provided to the Subject of personal data:

- Company Details as a Responsible Processor,
- List of personal data collected and identification of any of them that may belong to specific categories of personal data, according to the General Regulation or national law,
- Indication of the intention or possible forecast of any transmission (in this case the country of transmission is indicated and it is determined whether it concerns part or all of the personal data under processing),
- Reference to conservation and destruction periods,
- Reference to the confidentiality and assurance of the integrity of the personal data, throughout the processing,
- Explanation of the rights of the Subject of personal data (access, modification, opposition, revocation, portability, termination, etc.).

Consent must be given before the processing operation to which it relates. At the end of the retention period, the Subject of personal data is informed of the destruction of its data.

In Annexes II and III, respectively, are provided models of an agreement for the treatment and protection of employees' personal data of the Company and a statement of consent of a member of the Board of the Company, for the processing of personal data that concern it.

D. POLICY FOR THE PROTECTION OF THE RIGHTS OF THE SUBJECT OF PERSONAL DATA.

The management of the requests of the Subjects of the personal data, regarding their data and the processing to which they are subjected, constitutes a basic parameter of the general policy of the Company, regarding the protection of the security and the privacy of the personal data. For this reason, the Company adopts this policy, in order to ensure a complete and effective framework for the protection of rights and relevant response to the relevant requests of the personal data. This framework applies either in cases where the Company acts as the Controller or when it acts as the Executor.

1. Fundamental rights of personal data Subjects.

i. Right of access / information of the Subject of personal data

The personal data Subject is entitled to be informed by the Company as to whether its personal data are subject to processing or not. In case the personal data are processed, he will be given access to them or, if requested by the Subject, a copy of the data. In any case where personal data are collected from their Subject, the following information is provided to it (even if they have already been provided to the personal data Subject either prior to its consent or otherwise):

- The identity and full details of both the Controller and, if available, the Data Protection Officer.
- The purpose of the processing, as well as its legal basis. If the processing takes place because it is necessary for the purposes of the legal interests of the Company or a third party, these legal interests are disclosed.
- The categories of personal data that concern the processing and the type of processing.
- Recipients or categories of recipients to whom personal data have been or will be transmitted (if any), especially if they are in third countries or international organizations for which there is no adequate protection decision.
- **The retention period** of the personal data or, if this cannot be determined, the criteria to be taken into account for determining the interval.

- The existence of **a right to submit, to the Company, a request to access the personal data or to correct or delete the personal data or limit their processing**, a right to object to the processing in general or to specific forms of processing, as well as a right to data portability.

- When the legal basis of processing is the consent of the Subject of the personal data, the right to withdraw the consent without prejudice to the legality of the processing based on the consent before its withdrawal.

- The existence of a right to file a complaint to the Supervisory Authority.

- Whether the provision of personal data constitutes a legal or contractual obligation or requirement for the conclusion of a contract, as well as whether the Subject of personal data is required to provide personal data and what are the possible consequences of non-provision of such data.

- In any case where the personal data are to be processed for a purpose other than that for which they were collected, the Company provides the Subject of personal data, prior to such processing, with information on the purpose of the processing and any other necessary information.

In the event that personal data are not collected directly from their Subsidiary, the Company shall provide the personal data Subsidiary with any available information about their origin and, as appropriate, whether the data came from sources to which the IAEA has public access.

In any case, the right to information is subject to the restrictions of article 14 par. 5 of the General Regulation.

ii. Right to correction.

The Subject of the personal data has the right to submit an application to the Company, for the correction, without undue delay, of inaccurate personal data concerning it. The Company must satisfy this request, taking into account the purposes of processing. The Subject of the personal data also has the right to request the completion of incomplete personal data, inter alia, through a supplementary declaration.

The Company will announce any correction of the personal data to each recipient to whom this data was transmitted, unless this is not possible or if it involves a disproportionate effort or disproportionate expense.

iii. Right to delete (right to be forgotten).

The Company, as the Controller, will delete, without undue delay, personal data, if requested by the Subject of this data, if one of the following reasons applies:

- Personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

- The Subject of the personal data revokes the consent on which the processing is based and there is no other legal basis for the processing.

- It is established that there is no or that any legal reason for processing has disappeared.

- The personal data have been illegally processed in any way.

- The deletion of personal data is necessary in order to fulfill a legal obligation arising from EU or applicable national law.

- Personal data have been collected in the context of providing information society services directly by a child.

The right of deletion does not apply and the Company is not obliged to delete the personal data, when processing is necessary:

- ✓ For the exercise of the right to freedom of expression and the right to information,
- ✓ For the observance of a legal obligation which requires processing, under Union law or national law, or for the performance of a duty performed in the public interest,
- ✓ For reasons of public interest in the field of public health,
- ✓ For the purposes of archiving in the public interest, for the purposes of scientific or historical research or for statistical purposes, in accordance with Rule 89 par. 1 of the General Regulation, if the right of deletion is likely to make it impossible or to a large extent impede the achievement of purposes of such processing or
- ✓ To establish, exercise or support legal claims.

iv. Right to restrict processing.

The personal data Subject is entitled to ensure that the Company restricts the processing of its data, when one of the following reasons applies:

- The accuracy of the personal data is disputed by the Data Subject, for a period of time that allows the Company to verify the accuracy of the personal data,
- The processing is illegal and the personal data Subject opposes the deletion of personal data and instead seeks to limit their use,
- The Company no longer needs personal data for processing purposes, but these personal data are required by their Subsidiary to establish, exercise or support legal claims; or
- The personal data Subject has objections to the processing, pending its verification as to whether the Company's legal reasons prevail over the personal data Subjects' reasons.

When processing is restricted in accordance with the above, those personal data, other than storage, are processed only with the consent of the personal data Subject or for the establishment, exercise or support of legal claims or for the protection of the rights of another natural or legal in the interests of the public interest of the Union or a Member State.

The Subject of the personal data, which has secured the processing restriction, in accordance with the above, is informed by the Company before the removal of the processing restriction.

v. Right to personal data portability.

The Subject of the personal data has the right to receive the personal data that concern it and which it has provided to the Company, in a structured, commonly used and machine readable format, as well as the right to transmit the said data to another Processor, without objection from the Company, when:

- The processing is based on the consent of the personal data Subject or a contract to which the personal data Subject is a party or
- The processing of personal data is performed by automated means.

When exercising the right to portability of personal data, the personal data Subject has the right to request direct transmission of personal data, from the Company to another Processor, if this is technically feasible.

The right to portability of personal data is without prejudice to the right to delete them. This right does not apply to the elaboration of personal data that is necessary for the performance of a duty performed in the public interest.

The right to portability does not adversely affect the rights and freedoms of others.

vi. Right of objection.

The Subject of the personal data is entitled to object, at any time and for reasons related to his particular situation, to the processing of the personal data concerning him, which is based on reasons related to the performance of a duty performed in the public interest or fulfillment of purposes of the legal interests pursued by the Company, within the framework of its Articles of Association and the relevant legislation. The Company, in this case, no longer submits the personal data to processing, unless it demonstrates compelling and legal reasons for processing, which override the interests, rights and freedoms of the Subject of the personal data or for the establishment, exercise or support of legal claims.

The Subject of the personal data has the right not to be subject to a decision taken solely on the basis of an automated procedure, including profiling, which produces legal effects that affect or significantly affect it.

At the latest at the first communication with the subject of the personal data, the right of objection is explicitly indicated in it and is clearly and separately described from any other information.

2. Management of the requests of the Subject of personal data.

i. Receipt of requests and transmission to the Head of Protection of personal data.

The requests of the personal data Subjects are submitted by any appropriate means (by phone, e-mail, postal, etc.). In any case, when the request is submitted orally, the Subject of the personal data must complete a relevant written request.

Upon receipt of the request, the personal data Subscriber signs a receipt that his request has been received and that he has been informed of the contact details of the Data Security Officer (or - if any - of the personal data).

ii. Identification of the Subject of personal data

The identification of the personal data Subject is necessary for the exercise of its relevant rights and is the responsibility of the staff member, management bodies or services of the Company that carries out the processing or receives the request. The Police Identity Card, passport (if valid), driver's license, registration documents, health booklet and any other document that securely certifies the identity of the personal data subject are accepted as identification data.

In any case, if doubts are left regarding the identity of the personal data Subject, the member of the staff, management bodies or services of the Company that processes or receives the request, may request additional information or certification information.

If the request is not submitted in person but on behalf of the Subject of the personal data, a valid, strong and specific authorization must be submitted.

iii. Request log.

Each request submitted in accordance with this Chapter shall be recorded in a special file of requests kept by the Company, in accordance with the model provided in Annex III. Company, as Head of Processing. The Company always ensures the Data Security Officer (or - if any - the personal data) full access to the request log. The Data Security Officer (or personal data, if any) is responsible for ensures that the file of requests is properly maintained by the Company.

iv. Notification of requests to the Data Security Officer (or - if any - to the personal data). Evaluation of requests - Notification of the Subject of personal data.

Upon receipt of the request from the person organizing the staff, facilities or companies, corporate companies , delay, the request in the application to the Data Security insurer (or -by difference- to the personal data). Within blessing, the Data Security Superintendent investigates the Company, in terms of the availability of the request or in the personal nature of trust questions in one of the information provided exceptions, vectors and in terms of image presentation of the content of the image.

In any case, the Company informs the personal data Subject, regarding its request, no later than one month from the receipt of the request. This time can be extended for another month, in case the satisfaction of this is difficult for legal or practical / technical reasons.

No later than two months from the receipt of the request, the Company records, in the Request Log, the time and manner of satisfaction of the request or, in case of non-satisfaction, the reasons for which the request was not satisfied.

After two months from the submission of the request and if the request is not satisfied, the personal data Subject may request directly from the Data Security Officer a report on the reasons for the non-satisfaction of his request and the actions he has taken or intends to take himself for the protection of the relevant rights of the Subject of personal data.

In case the non-satisfaction of the request of the Subject of the personal data constitutes a violation of the General Regulation, the Data Security Officer informs the Subject of the personal data about his right to compensation, according to article 82 of the General Regulation.

The provisions of this sub-chapter, regarding the policy of management of requests of the personal data Subjects, are applied accordingly in the cases where the Company acts as the Executor of the Processing.

E. PERSONAL DATA VIOLATIONS POLICY.

A necessary condition for ensuring an adequate level of protection of the security and confidentiality of personal data is the formulation and faithful observance, by the Company as Responsible Processor (or as Executor of Processing), of a policy framework for the effective treatment of any breach, in accordance with the relevant requirements of the General Regulation and national legislation.

1. Concept of personal data violation

According to the relevant definition of the General Regulation (article 4 par. 12), a breach of personal data is considered any breach of security that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or submitted in another way of editing.

For systematic reasons and for the better organization of the means and the procedures for dealing with them, the violations are divided into the following categories:

- Violation of confidentiality: Unauthorized or accidental or illegal disclosure or access to personal data.

- Availability breach: Unauthorized or accidental or illegal destruction or loss of access to personal data.

- Integrity breach: Unauthorized or accidental or unlawful alteration or alteration of personal data.

Depending on the circumstances, a breach may fall into more than one of the above categories.

2. Personal data violation management

i. Detection - detection of the violation

The detection and detection of a personal data violation can be done either by a member of the staff, organs or services of the Company or by the Data Security Officer, or by the executor of the processing or by the personal data Subject itself.

ii. Notification of the Data Security Officer (or - if any - of the personal data Officer) - Violation response team.

As soon as any violation of personal data is detected and / or detected, the Data Security Officer is notified, in order to take the appropriate measures to investigate and deal with the violation.

Simultaneously with the notification, a team to deal with the violation is formed, which is staffed by at least:

- The Data Security Officer (and - if any - the Data Security Officer),
- The Legal Advisor of the Company and
-
- The Chief Executive Officer and / or the Chairman of the Board of Directors of the Company or an executive member of the Board of Directors as a deputy.

The team has overall responsibility for managing the incident, handling relevant investigations and taking appropriate action to address the breach.

iii. Object of research.

Investigations carried out under the responsibility of the violation response team shall cover at least a) the causes of the violation (intentional leakage of personal data, negligence of the responsible staff member, organs or services of the Company, cyber-attack, etc.), b) the person / persons (c) the possible

consequences and dangers for the rights and freedoms of the personal data Subject, in order to determine whether the incident requires notification to the Personal Data Protection Authority.

Elements to be taken into account for risk assessment:

- The type of violation (e.g. if it is an illegal disclosure of personal data to third parties, the risk is more serious than in the case of an accidental loss of access).

- The nature, sensitivity and volume of the personal data that were violated (e.g. the risk is more serious if they are personal data that fall into specific categories or if a combination of personal data was violated and not individual ones).
-
- Possibility to identify the Subject of the personal data (the extent to which the person who caused the breach can identify the Subject of the personal data that was violated or link the personal data to other information to identify the Subject).

- Significance of the consequences of the breach on the personal data Subject (for the determination of which the type of damage is taken into account -material damage and / or non-pecuniary damage- and the duration of its consequences).

- Special characteristics of the Subject of personal data (the risk is more serious and the consequences are heavier if the Subject personal data belongs to sensitive or vulnerable categories - e.g. if he is a child).

- The number of personal data Subjects affected (the greater the risk and the wider the impact, the more personal data Subjects affected by the breach).

iv. Taking measures to address the violation - Notification.

Following the investigation of the causes, the culprits of the violation of the personal data and the assessment of the risks and the extent of the consequences, the appropriate measures must be taken without delay to address it and to limit its effects.

Based on the assessment of the severity of the risk and the extent of the impact:

- If the risk is low, the case can be closed as soon as the violation is removed and any consequences are addressed. In any case, the Data Security Officer (or - if any - the Data Protection Officer) must record each breach in the personal data Breach Record.

- If the risk is high, the Data Security Officer (or Data Protection Officer_ must report the breach to the Personal Data Protection Authority and, if necessary, to the Data Subjects who have been breached.

  The notification to the Personal Data Protection Authority is made without delay and not later than 72 hours from the time at which the violation of the personal data was realized. In the event that the notification is made after this time limit, the delay must be specifically justified.
  A model notification form is attached to Annex V to the Personal Data Protection Authority.

According to Article 33 of the General Regulation, the notification to the Personal Data Protection Authority should at least:

- ✓ Describes the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects affected, as well as the categories and approximate number of personal data files affected,

- ✓ Announces the name and contact details of the Data Security Officer (or Data Officer, if any) or other contact point, from which more information can be obtained,

- ✓ Describes the possible consequences of the violation of personal data,
- ✓
- ✓ Describes the measures taken or proposed to be taken by the Company, to address the violation of personal data, as well as, where appropriate, measures to mitigate any adverse consequences.

In case it is not possible to provide all the information at the same time, it can be provided gradually, without undue delay.

v. Report of personal data violation to the Data Subject.

In cases where the violation of personal data may expose to a high risk the rights and freedoms of individuals, the Company promptly notifies the violation to the Data Subject. This notice shall clearly describe the nature of the data breach, the name and contact details of the Data Security Officer (or - if any - the Data Officer) or other contact point from which more information can be obtained, describes the possible consequences of the breach, as well as the measures taken or to be taken to address the breach and mitigate any adverse consequences.

The notification of personal data violation is made directly to the personal data Subject, unless this would involve a disproportionate effort. In this case, a public announcement can be made.

vi. Personal Data Violation File.

Any violation of personal data found, regardless of its severity and the risks involved, is recorded in a special Data Violation Record, which is kept by the Data Security Officer (or the Data Protector, if any).