ELLAKTOR S.A.

DATA PROTECTION POLICY

December 2019

1. Legal framework for data protection

The General Data Protection Regulation (EU) 2016/679 (GDPR) and Law 4624/2019 constitute the legal framework, which governs the processing of personal data and ensures the protection of the rights and freedoms of natural persons when their data is processed. The purpose, inter alia, is to ensure that any processing of personal data takes place with the knowledge of the natural persons concerned and that all the principles and conditions of legality laid down by the GDPR and applicable national law are met.

2. Definitions

2.1. Personal data: Any piece of information by which a natural person can be identified directly or indirectly (data subject). Such information is a name, an ID number, a tax registration number, a social security registration number, a postal address, a telephone number or an e-mail address, a car registration number, location data, a face image that is received through a closed-circuit television or online identifiers. In addition, personal data can be one or more factors that are specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of a natural person if through them the natural person can be identified. The data of legal entities are not personal data and are not protected by the relevant legislation.

2.2. Special categories of personal data: Personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

2.3. ELLAKTOR Group (the Group): All companies that are included in the annual consolidated financial statements of the parent company ELLAKTOR S.A.

2.4. Group Data Protection Officer (DPO): The person appointed by ELLAKTOR Group to exercise independent supervision over any matter relating to the processing of personal data. In particular, the DPO informs and advises the Group, its executives and staff, monitors compliance with the GDPR and the current national legal framework for data protection, assists in the formulation of relevant policies and procedures and monitors their implementation, and is the point of contact of the Group for the Hellenic Data Protection Authority.

3. General Principles observed by the Group

3.1. The companies of the ELLAKTOR Group are bound to fully comply with the obligations and other provisions of the GDPR and applicable national law during the processing of the personal data of the executives, the staff, the associates, the suppliers, the shareholders, the bondholders or the customers of the Group as well as every third natural person, in the exercise of their legal activities and the provision of their services. Compliance with the current legal framework for data protection is a key priority of the Group. For this purpose, the Group implements all appropriate organizational and technical measures and procedures for data protection and respect for the rights of natural persons to which they refer.

3.2. The Group is bound not to process special categories of personal data, except health data, provided there is a relevant legal obligation, and is always taking the appropriate technical and organizational measures for the security of this data and for the access to them only by specifically authorized competent persons bound by duty of confidentiality.

3.3. The executives, the staff as well as all external associates or any third parties that cooperate or perform works on behalf of the Group, who, within the framework of their responsibilities and duties, have access to personal data that are processed in the framework of the Group's legal activities, are expected to have read, understood and complied with this Policy.

3.4. Violation of the principles set forth in this Policy as well as the provisions of the GDPR and the applicable national legal framework will be dealt with in accordance with the Group's Code of Conduct in addition to any other legal sanctions that violation of the law may result in.

3.5. No third party may have access to personal data belonging to the Group without having first concluded a data confidentiality agreement, which imposes on the third party no less burdensome obligations than those to which the Group is bound to comply with, and entitles the Group to monitor third parties for their compliance.

3.6. The Group keeps a record of the processing activities in which the processing activities appear with their specific characteristics that refer to the purpose, the legal basis, the categories of data subjects and the categories of personal data that are subject to processing, the potential recipients of this data, the data retention time, possible data transfers outside the European Economic Area and the technical and organizational measures applied for the security of personal data. This file is kept by the Coordinating Committee for Data Protection of the Group under the supervision of the DPO and is made available to the Hellenic Data Protection Authority upon its request.

4. Responsibilities and roles

4.1. ELLAKTOR Group is Controller for the processing of personal data in accordance with the GDPR, Law 4624/2019 and this Policy.

4.2. The Management and all those who play a managerial or supervisory role within the Group are responsible for encouraging the implementation of proper personal data management procedures and they define the responsibilities and obligations reflected in the individual job descriptions.

4.3. The DPO carries out its duties with complete independence, does not receive any mandates for the exercise of its duties and refers to the highest administrative level of the Group for any matter concerning the management of personal data and ensuring compliance with personal data protection legislation.

4.4. The Group ensures that the DPO participates in all issues related to the protection of personal data, supports the DPO in the performance of his duties by providing him the necessary resources for the performance of these duties and the maintenance of his expertise and ensures that he can access the personal data and the processing operations of the Group.

4.5. The DPO is assisted by the Coordinating Committee for Data Protection of the Group, which is responsible for coordinating the actions required in relation to the Group's compliance with the requirements of the GDPR and the current national legal framework, and for assisting in general the DPO in the exercise of his duties.

4.6. The Coordinating Committee for Data Protection consists of:

(a) The Chief Human Resources Officer,

(b) The Chief IT Officer,

(c) The Director of Group's Administrative Services,

(d) The Group Head of Compliance Officer and

(e) The Chief Legal Adviser of the Group.

4.7. The Coordinating Committee for Data Protection is responsible for maintaining the Group's Record of Processing Activities as well as all relevant policies, procedures, contract texts, information texts, impact assessments and any other evidence that demonstrates the Group's compliance with the GDPR and the national legislation on the protection of personal data. In addition, it is also responsible for maintaining the register of requests for the exercise of the data subjects rights and the register of notifications of personal data breaches.

4.8. The DPO is the first point of contact with the employees and other data subjects for the exercise of their rights in relation to the processing of their personal data, and for the provision of clarifications on any issue concerning the protection of personal data within the Group.

4.9. Compliance with the legislation on the protection of personal data is the responsibility of all those executives and employees of the Group who process personal data and who are bound by a duty of confidentiality.

5. Principles related to processing of personal data

5.1. The processing of the personal data of the Group is carried out in accordance with the principles of protection of personal data, as defined in article 5 of the GDPR and are described in the record of processing activities of the Group, and are the following:

(a) Personal data shall be processed lawfully, fairly and transparently (principle of lawfulness, fairness and transparency).

(b) Personal data shall be collected only for specified, explicit, clear and legitimate purposes and shall not be processed in a manner that is incompatible with or in excess of these purposes (principle of purpose limitation).

(c) The personal data collected shall be adequate, relevant and limited to what is strictly necessary, for the purposes for which they are collected, kept and processed (principle of data minimization).

(d) Personal data shall be accurate and up-to-date and efforts shall be made to erase or rectify it without delay (principle of accuracy).

(e) Personal data shall be kept in such a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (principle of storage limitation).

(f) Personal data shall be processed in a manner that ensures necessary security and protection against unauthorized or unlawful access, disclosure, loss, destruction or damage (principle of integrity and confidentiality).

(g) The controller must always be able to demonstrate compliance with the requirements of the GDPR (principle of accountability).

6. Rights of data subjects

6.1. The data subjects have the following rights regarding the processing of personal data maintained and processed by the Group:

(a) The right to be informed of the categories of personal data that are being processed as well as of the purposes, the legal basis, the potential recipients and the general conditions for the processing of their personal data.

(b) The right of access to their personal data that are being processed and the conditions of such processing.

(c) The right to rectification of inaccurate data concerning them or to have incomplete data completed.

(d) The right to erasure their data (right to be forgotten), provided that the terms and conditions of Article 17 of the GDPR are met.

(e) The right to restriction of processing of data for the reasons and under the conditions of Article 18 of the GDPR, in particular where:

(i) The accuracy of the personal data is contested by the data subject and until the Group verifies the accuracy of that data.

(ii) The processing is unlawful, but the data subjects oppose the erasure of the data and request the restriction of their use instead.

(iii) The Group no longer needs the data, but this data is required by the data subjects for the establishment, exercise or defence of legal claims.

(iv) The data subjects have objections to the processing during the period of time that elapses until it is verified whether the legitimate grounds presented by the Group override those of the data subject.

(f) The right to data portability. In particular, the data subjects have a) the right to receive the personal data concerning them and which they provided to the Group, in a structured, commonly used and machine-readable format, as well as b) the right to transmit those data to another controller without the Group having the right to hinder, when the processing is based on the consent of the subjects or on a contract and is carried out by automated means.

(g) The right to object to the processing of their data on grounds relating to their particular situation, including profiling, under the conditions of Article 21 of the GDRP. If personal data is processed by the Group for the promotion of corporate - commercial purposes (marketing), the data subjects shall have the right to object to the processing of their data for the above purposes, which includes profiling that is related to direct marketing.

(h) The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or significantly affect them in a similar way. The exercise of the above right is not allowed (i)if the corporate decision is necessary for entering into, or performance of, a contract between the data subject and the Group, (ii)if this is allowed by law or (iii)if it is based on the data subjects' prior explicit consent.

6.2. Data subjects may exercise the above rights by submitting a request as described in the Procedure for the Exercise of the Rights (Annex I). The Group shall be bound to respond to the relevant requests of the subjects in accordance with the provisions of the GDPR, the applicable national legislation and the aforementioned internal procedure.

7. Data security

7.1. All executives and employees of the Group are responsible for ensuring that the personal data kept and processed by the Group are kept secure and are not disclosed or transferred to any third party, unless the third party is authorized by the Group to receive and process such information in the context of (a) the legal activities of the Group and provided that it has entered into a corresponding confidentiality agreement or (b) there is a relevant legal obligation by law or by a court decision.

7.2. Executives and employees of the Group have access to personal data based on the needs of their duties and responsibilities and the access rights that have been given to them.

7.3. The Group takes all appropriate technical and organizational steps for the security of personal data that it keeps and processes. In particular, inter alia, personal data must be kept in a locked room with controlled access and / or in lockable drawers or lockable file cabinets, and, if in electronic form, be password protected and when stored on removable media must be encrypted in accordance with the requirements of the relevant internal policies of the Group.

7.4. The Group implements, both at the time of determination of the means for processing and at the time of the processing itself, appropriate technical and organizational measures, which are designed to implement data-protection principles and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and to protect the rights of data subjects (data protection by design).

7.5. The Group implements appropriate technical and organizational measures for ensuring that, by default, only personal data, which are necessary for each specific purpose of the processing, are processed.

7.6. In case of a personal data breach, the Group without undue delay informs the Hellenic Data Protection Authority, unless the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons, providing all necessary information and documentation. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Group shall communicate the personal data breach to the data subjects, unless such communication requires a disproportionate effort, or in the meantime the Group has applied appropriate technical and organizational protection measures to the personal data affected by the breach and rendered them unintelligible to any unauthorised person, or in the meantime the Group has taken measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.

8. Storage period and destruction of personal data

8.1. The Group does not keep personal data in a form that allows the identification of data subjects for a period longer than what is necessary in relation to the purposes for which the data were collected.

8.2. Personal data, whether kept in electronic form or in a physical file, are erased after the expiration of their storage period, which has been determined depending on the category of data and the purpose of processing in the context of the respective activity, according to the Data Retention and Destruction Procedure (Annex II).

8.3. The Group has the ability to store personal data for a longer period than the specified storage period, if the personal data is to be processed solely for archiving purposes, for scientific or historical research purposes or for statistical purposes, without prejudice to the implementation of the appropriate technical and organizational measures to safeguard the rights and freedoms of data subjects.

9. Transfer of data outside the European Union

9.1. The Group does not transfer any personal data, which keeps and processes, to countries outside the European Union (EU) unless there is an appropriate level for the protection of the data subjects based on a relevant European Commission decision or one or more of the safeguards or exceptions set out in Chapter V of the GDPR are valid.

9.2. If, in the context of its legal activities, there is a need to transfer personal data outside the EU, the Group selects the appropriate mechanisms for the lawful transfer fully complying with the GDPR and informs accordingly the data subjects.

9.3. The DPO checks whether the legal conditions for the transfer of data exist.

10. Final provisions – approval and revision of the Policy

10.1. Under the responsibility of the Group Head of Compliance, the Data Protection Policy is posted updated on the Group website www.ellaktor.com

10.2. The Data Protection Policy is approved by the CEO, overviewed on an annual basis and reviewed whenever necessary. The DPO is responsible for preparing and proposing revisions to this Policy in cooperation with the Coordinating Committee for Data Protection if necessary.

ANNEX I

Procedure for the Exercise of the Rights

A. Introduction

The companies of ELLAKTOR Group process personal data of executives, employees, associates, suppliers, shareholders, bondholders or their customers as well as any third party natural person in the context of the exercise of their legal activities and the provision of services (data subjects), in full compliance with applicable personal data protection legislation.

Data subjects have a number of rights, which they can exercise by submitting a request to the Group. In particular, data subjects have the right to access their personal data kept by the Group including the right to request a copy of this data and, where required, the updating of the data. They, also, have the right to correction, erasure, restriction of processing, portability of their data and to objectto the processing as well as to the automated individual decision making (profiling), provided that the corresponding conditions required by law are met.

The purpose of this procedure is to determine how the above rights are exercised as well as the roles of the staff members of the Group who are authorized to manage the relevant requests by the data subjects.

B. General procedure for the exercise of the rights

B.1. Submission of the request and verification of the applicants' identity

Data subjects may submit their requests for the exercise of their rights by completing the special form[1], which is attached to this Annex and can be submitted either by post to the offices of the Group (ELLAKTOR S.A., 25 Ermou street, 14564 Kifissia) or electronically at the e-mail address dpo@ellaktor.com. If the subject communicates with the Group by phone, he/she is provided with this information.

Each request is registered in the Register of Data Subject Requests, which includes all the details of each request (submission date, request processing, additional information necessary to the handling of the request, the response and the relevant date). Responsible person for the maintenance and updating of the Register is the Data Protection Officer in cooperation with the competent employees of corresponding departments.

The Group must verify the identity of the data subject at the time he/she submits a request in order to proceed with the handling of the request. If the request is submitted via email, an email is sent to the sender's email address and he/she is asked to confirm that he/she has submitted the request. The reply is sent to the same email address. If the request is submitted in writing, the competent employee confirms the identification of the subject with the presentation of an identity card (or residence permit or passport if he/she is a foreigner) of the subject.

The subject declares in the application form whether he/she wishes to receive the answer from the Group's offices by presenting an identity card or he/she wishes the answer to be sent to a specific postal or electronic address.

B.2. Procedure for examining the request

The request is notified to the competent department, which undertakes to inform the DPO. The request is then examined by the DPO in collaboration with the competent department in order to review it and formulate the appropriate response.

[1] Application form for data subject rights.

B.3. Procedure fees

The relevant information and any announcement, as well as all the actions of the Group, following the relevant requests, are provided free of charge.

B.4. Response time

The Group completes the review of the request and responds to the subject without delay and in any case within 30 days of receipt of the request. This deadline may be extended by a further two months if required, if e.g. the request is complex or there are a large number of requests to be handled. In case of extension, the Group must inform the subject before the expiration of the initial 30 days of the reasons for the delay by e-mail or postal letter. The responsible person for communication with the subject is the DPO.

B.5. Obligation to notify the recipients

In any case where the Group satisfies the request of the subject, it announces any correction, erasure restriction of processing carried out to each recipient to whom the data were disclosed, unless this is proved to be impossible or if it would involve disproportionate effort. Upon request by the data subject, the Group informs him/her about these recipients through the DPO.

C. Procedure for exercising specific rights

C.1. Right of access

The Group as Controller provides confirmation to the data subjects as to whether or not the personal data concerning them are being processed and, where that is the case, satisfies the right of access to such data. The answer must contain at least the following information:

(a) the purposes of the processing;

(b) the categories of personal data collected;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations, and the legal basis on which such transfer is made;

(d) where possible, the envisaged period for which the data will be stored or, if not possible, the criteria used to determine that period;

(e) the existence of the relevant rights;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) where applicable, the ability to make automated decisions that produce legal effects or significantly affect the subject, including profiling, including those based on specific categories of data, and the logic followed.

Restrictions on the right of access

The satisfaction of the right of access and the receipt of a copy of the data should not adversely affect the rights or freedoms of others, such as the professional secrecy or intellectual property rights and in particular the copyright protecting the software. However, the above should not result in the refusal to provide any information to the data subject.

When the processing concerns large quantities of information, the Group may request from the subject further specification of the requested information or specialization of the request.

C.2. Right to rectification

The Group is obliged, upon a relevant request by the data subject, to rectify inaccurate personal data concerning him/her. In addition, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement.

If the accuracy of the data is contested by the data subject, the latter has the right to obtain from the Group the restriction of processing for a period of time that enables the Group to verify the accuracy of the personal data.

C.3. Right to erasure

The Group has an obligation at the request of the data subject to erase personal data concerning him/her, if one of the following reasons applies:

(a) personal data are no longer necessary in relation to the purposes for which they were collected or processed;

(b) the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing;

(c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes, including profiling;

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased, based on a legal obligation to which the Group is subject;

(f) the personal data have been collected in relation to the offer of information society services directly to a child.

Restrictions on the right to erasure

Data are not erased when the processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Group;

(c) for scientific or hisrorical research purposes or statistical purposes in so far as the erasure is likely to render impossible or seriously impair the achievement of those objectives;

(d) for the establishmenet, exercise or defence of legal claims.

The weighting is DPO's responsibility.

In any case, the Group must notify the reasoned decision to the requestor, informing him/her, especially in case of refusal, of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

C.4. Right to restriction of processing

The Group has the obligation to ensure the restriction of processing to the data subject, where one of the following reasons applies:

(a) the accuracy of the personal data is contested by the data subject, for a period of time enabling the Group to verify the accuracy of the data;

(b) the processing is unlawful and the data subject opposes the erasure of the data and requests the restriction of their use instead;

(c) the Group no longer needs the data, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing, pending the verification whether the legitimate grounds of the Group override those of the data subject.

If the request is valid, restrictive methods could include, inter alia, the temporary movement of the selected data to another processing system, the removal of accessibility from users, or the temporary removal of published data from a web page. The fact that data processing is restricted should be noted in the system. A data subject who has obtained restriction of processing in accordance with the above, shall be informed before the restriction of processing is lifted.

C.5. Right to data portability

The Group has the obligation upon request of the data subject to provide the personal data concerning him/her and which the subject has provided in a structured, commonly used and machine-readable format, as well as to satisfy the right of the subject το transmit those data directly to another controller without objection, when the following conditions are met:

(a) the processing is based on the consent of the subject or processing is necessary for the performance of a contract to which the subject is a party; and

(b) the processing is carried out by automated means.

The data falling within the scope of the right to portability must be:

(a) personal data that have not been anonymized; however, data that have been pseudonymized and can be used for the identification of the subject are within scope.

(b) personal data that the subject has provided to the Group, but also observed data that have been provided by the subject through the use of a service or device (e.g. search history, location and position data); on the other hand, "inferred data" and "derived data", i.e. those created by the Group based on the data provided by the data subject, are not included.

Restrictions on the right to data portability

This right does not apply to the transmission of data containing personal data of other (non-consenting) subjects to a new controller. For this reason, the Group must apply mechanisms for obtaining consent from any other subjects involved in order to facilitate the transmission in cases where these third parties are willing to consent.

Professional secrecy or intellectual property rights, and in particular copyright protecting the software must be taken into account before responding to a data portability request. However, the above should not result in the refusal to provide any information to the data subject. It is also pointed out that the Group cannot reject requests for data portability on the basis of violation of another contractual right (e.g. outstanding debt, or commercial dispute with the data subject).

The Group has no specific obligation to check and verify the quality of the data before they are transmitted, however these should be accurate and up to date.

C.6. Right to object

The Group has the obligation not to process personal data if the data subject objects, on grounds relating to his/her particular situation to processing of personal data concerning him/her, in cases where the processing is based on:

(a) the performance of a task carried out in the public interest or in the exercise of official authority vested in the Group;

(b) the legitimate interests pursued by the Group or by a third party, including profiling.

When data are processed for direct marketing purposes, the data subject has the right to object to processing for such marketing at any time.

Where data are processed for scientific or historical research purposes or statistical purposes, the data subject has the right to object to processing, on grounds relating to his/her particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

The DPO makes the necessary weightings for the review of the request.

Pending the verification whether the legitimate grounds of the Group override those of the data subject, the subject has the right to obtain the restriction of the specific processing.

C.7. Automated individual decision-making, including profiling

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

The Group does not in principle perform automated processing, including profiling, which produces legal effects for the data subject, unless:

(a) it is necessary for entering into, or performance of, a contract with the data subject;

(b) it is authorized by law; or

(c) it is based on the data subject's explicit consent.

In any such case, the Group implements suitable measures to safeguard the specific information of the data subject, the right to ensure human intervention, the right to obtain human intervention, the right of the subject to express his/her point of view, the subject's right to receive a reasoned decision taken in the context of that assessment and the right to contest the decision.

The DPO is responsible for receiving and answering relevant questions, which are submitted through the application form.

In case the legal basis for the processing is consent, it is freely revocable at any time.

APPLICATION FORM FOR DATA SUBJECT RIGHTS

in accordance with the provisions of Chapter III
of the General Data Protection Regulation (EU) 2016/679

To
ELLAKTOR Group
25 Ermou street, 145 64 Kifissia
dpo@ellaktor.com
To the attention of the Data Protection Officer (DPO)

Data subject information

Name and Surname:

Father's name:

ID number:

Postal address:

Telephone numbers:

E-mail:

Contested right

- ☐ Right of information and access
- ☐ Right to rectification
- ☐ Right to erasure
- ☐ Right to restriction of processing
- ☐ Right to data portability
- ☐ Right to object
- ☐ Automated individual decision-making

Subject matter of the request

1. Relation to ELLAKTOR Group

2. Categories of data *(please, specify)*

3. Processing activities *(please, specify)*

4. Description of the request

Desired way of communication

- ☐ E-mail
- ☐ Postal communication
- ☐ Telephone communication (for the receipt of the answer)
- ☐ Other – please specify: _____

Place: _____ Date: ___ / ___ / _____

Requestor's signature

_____

ANNEX II

Personal Data Storage and Destruction Procedure

A. Introduction

This procedure provides information and describes the Group's obligations regarding the safekeeping and secure destruction of personal data in accordance with applicable data protection legislation.

B. Storage of data

B.1 Determination of retention time of personal data

The Group retains personal data only for the period of time that is necessary as it is specifically determined by the purposes of the activities and the categories of data. The following are taken into account for the determination of the retention periods of personal data:

(a) the purpose of collection and processing;

(b) the legal basis for processing;

(c) the type of personal data (simple or specific categories of data);

(d) the categories of data subjects;

(e) the business needs of the Group.

In cases where it is possible to accurately determine the retention period, this is explicitly mentioned.

In cases where it is not possible to clearly and in advance determine the retention time of the data, the specific criteria that shape and determine this time are pointed out, thus ensuring the regular review of the data and their retention time based on the mentioned criteria.

In addition, personal data may be retained for a longer period of time, provided that they are intended for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes, while appropriate technical and organizational measures shall be implemented for the protection of the rights and freedoms of data subjects, according to the GDPR.

B 2. Allocation of responsibilities

The Coordinating Committee for Data Protection, in cooperation with the DPO, is responsible for:

(a) the formation, completion or modification of personal data retention times, whenever deemed necessary and in accordance with the requirements arising from the corporate activity of the Group or from requirements imposed by law;

(b) the annual review and updating of personal data retention times;

(c) monitoring the Group's compliance with this procedure; and

(d) informing the Group employees about their responsibilities regarding the maintenance of records and data as well as any changes that occur in connection with these responsibilities.

All employees of the Group are responsible for:

(a) creating and maintaining files related to the object of their work;

(b) the storage of files on approved storage means;

(c) compliance with the present procedure and the Group's file management procedures; and

(d) the destruction/deletion of files that have reached the end of their retention period.

C. Destruction of data

At the end of the retention period of personal data, they must be destroyed in a safe way. A safe way of destruction is considered to be any set of procedures and a set of measures that, after their complete implementation, make it impossible to identify the data subjects in any way, and, in any case, excluding the possibility of recovering these data by any means.

For the selection of the appropriate way of safe destruction, the means used for the storage and processing of personal data are taken into account, e.g. files in print, files in electronic format, files in any other format.

As indicative ways of destruction, depending on the means of retention and processing, are determined for the data in printed form the shredding, mashing-recycling and incineration, while for the data in electronic or other form the alteration of the data through their replacement with random characters (overwrite), formatting and natural disaster.

The Group may entrust the safe destruction of personal data to a third party or company that will act on its behalf, acting as processor, while complying with the provisions of the data protection framework regarding the assignment of processing, including the obligation to enter into a contract a minimum content, as defined in the applicable provisions, and the implementation of appropriate technical and organizational measures for data security until their final destruction.

Specifically for personal data governed by a special privacy regime provided by law (e.g. medical confidentiality), the Group must carry out the destruction itself (without assigning it to a processor) to fully ensure their confidentiality by any unauthorized access. In cases where this is particularly difficult or impossible, the assignment to a processor is organized in such a way that the Group has the overall supervision of the destruction process, as indicatively, either through its implementation within its premises, or in the presence of an authorized Group's employee.

Irrespective of the method of destruction chosen, after the completion of the process, a destruction protocol is drawn up, the minimum content of which includes the following information: date of destruction of personal data, description of the personal data, method of destruction, name of the employee designated as responsible for destruction and case of assignment, detailed information about the processor.