COMPANY LETTERHEAD

Part A – APPOINTMENT OF THE PERSONS AUTHORIZED TO PROCESS PERSONAL DATA
relating to (insert company name)

Pursuant to EU Regulation 2016/679 "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data"

The persons who process personal data, in carrying out their activities within (insert company name) are authorized to process personal data, pursuant to and for the purposes of articles. 28 and 29 of EU Regulation no. 679/2016.

Based on this assignment, each person authorized to process personal data is required to comply with the specific instructions given by (insert company name).

In particular, basing on the obligations of confidentiality and security imposed by the aforementioned legislation, it will be under the responsibility of each person authorized to process personal data to not disclose or disclose to third parties the processed data, except in the cases permitted by the specific provisions of the Law and, in any case, in compliance with the internal rules and procedures, issued by the Data Controller/Data Processor of (insert company name).

The categories of data subjects, whose personal data are accessed and processed by the persons authorized to process personal data (both IT and paper), strictly relevant to the performed tasks and for the purposes shown below by (insert company name), in compliance with the fundamental principles established by the Regulation, are the following:

- Employees and Crew (if applicable) for the following processing purposes:
  - Internal management of the staff
- Candidates for the following processing purposes:
  - Selection and recruitment procedures
- Suppliers and Customers for the following processing purposes:
  - Management of contracts
- Board members for the following processing purposes:
  - Management of contracts
- Visitors for the following processing purposes:
  - Completion of access procedures
  - Access to Internet facilities
  - Security

In particular, each person authorized to process personal data has to take care of the following:

- the methods of processing have to be compliant with the rules established by the Regulation;
- the ensuring of the maintenance of all necessary measures to avoid the increase of risks of destruction or loss of data, of unauthorized access or of not permitted processing, or of processing different from the purposes of the collection;
- the communication of personal data is avoided outside the hypotheses and modalities permitted by the Regulation; in particular, personal data should not be communicated to third parties or, in any case, to subjects that cannot be identified with certainty as having the right;
- special categories of data, as defined by art. 9 of the Regulation, are subject to processing only with the explicit consent of the data subject and in strict and timely compliance with the Regulation;
- any other legislative or regulatory provision on the matter is in any case observed.

Each person authorized to process personal data is also required to comply with the procedures relating to the Company's prescribed safety measures, including the instructions set out in Part B of this document.

THE DATA CONTROLLER

(insert company name).

_____

Signature for receipt and acceptance

THE PERSON AUTHORIZED TO PROCESS PERSONAL DATA

_____

Date _____

Parte B – OPERATING INSTRUCTIONS TO THE PERSONS AUTHORIZED TO PROCESS PERSONAL DATA

1. PREMISE

The EU Regulation 2016/679 "on the *protection of natural persons with regard to the processing of personal data and on the free movement of such data*" in order to ensure that the processing is carried out in the respect of the rights of data subjects, provide that the Data Controller and the Data Processor has to impart specific operating instructions to the persons that, in the exercise of their tasks, are authorized to process personal data, both by computer systems and by paper documents (art.28).

These instructions, as well as other security measures, aim to minimize the following risks:

- destruction or loss of personal data, even if accidental;
- unauthorized access;
- processing not allowed or not compliant with the collection purposes.

Below there are the main rules that all the persons authorized to the processing must follow in their daily activities and, especially, when they concern the process of personal data.

2. DEFINITIONS

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Genetic data: personal data relating to the inherited or acquired genetic characteristics of a natural person, which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Biometric data: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Data concerning health: personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

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

Data Processor: natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Third Party: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Data Subject: the natural or legal person, bodies or association to which personal data refer.

Communication: giving personal data knowledge to one or more specific subjects other than those involved, by the representative of the Owner in the territory of the State and by Data Controller, in any form, including making data available or by consulting them.

Anonymous data: data that originally, or because of processing, cannot be associated with an identified or identifiable individual.

Blocking the storage of personal data with temporary suspension of any other processing operation.

3. PROCESSING OF PERSONAL DATA

3.1 CREATION OF ARCHIVES RELATED TO NEW CATEGORIES OF DATA SUBJECTS

The persons authorized to process personal data are authorized to manage exclusively the archives of personal data identified in the respective appointment letters. The Data Processor must previously authorize any possible creation or use of archives concerning new categories of data subjects, as well as the execution of further processing in addition to those already existing.

3.2 PROCESSING CONTEXT ALLOWED

One of the focal point of the Regulation is that which provides that the processing of personal data must be declared in details to the data subject and it has to be carried out in the extent of what declared. In other terms, if the data subject is informed about the methods of the processing of his own personal data, that information fixes the limits of the processing.

In addition to identify the processing operations in their appointment letter, each person authorized to process personal data will find further information on the processing permitted to him, knowing the

information provided to data subject. It is clear that each person authorized to process personal data will take care to evaluate more carefully the information that most directly concerns his activity.

A specific attention must be devoted to the hypothesis of communication or dissemination of data. In other words, whenever the possibility of disclosing (in any form or way) personal data is presented, it is necessary to carry out the following checks:

- verification of the legitimacy of disclosure in light of the information provided to the data subjects;
- verification of any legislative provision that allows disclosure or make it mandatory.

In relation to the data subject's categories for which the processing is authorized, the data will be communicated exclusively to external subjects indicated by (insert company name).

The Data Controller or the Data Processor must previously authorize any different hypothesis of communication or even of data diffusion from time to time.

3.3 DATA UPDATE AND ACCURACY

The person authorized to process personal data must pay particular attention to the accuracy of the data processed and to update them.

4. INSTRUCTIONS FOR DATA PROCESSING WITH ELECTRONIC INSTRUMENTS

All those who, in any capacity, access the Company's information system, whether or not connected to the network, or who keep any personal data relating to the Company and not intended for dissemination, must comply with the following.

In particular, it should be noted that:

- Access to any type of processing of personal data with electronic tools is always subject to the passing of a computer authentication procedure that provides for the insertion by the operator of his own identification code (user name) and a password reserved and known only by the himself.
- The subsequent access to electronic tools necessary for the processing of personal data for the proper execution of your task is ensured by the configuration on your profile of further levels of authentication credentials.
- The password represents the first barrier in a strategy of selective access to personal data, and therefore a password selected with unsatisfactory criteria can lead to the compromise of the entire information network of the Company.

For this reason, each person authorized to process personal data is responsible for the secrecy of the password associated with his identification code and, therefore, is required to take all appropriate initiatives to ensure the security of it.

4.1 GUIDE-LINES FOR THE CONSTRUCTION OF PASSWORDS

In order to ensure compliance with the provisions of the Regulation, (insert company name) has provided access password to systems with a minimum length of 8 characters. It has also been set an expiration of the password of the employees every 6 months for the common personal data and every 3 months for the ones belonging to special categories.

The Company's policies recommended on the choice of passwords, in accordance with the international best practices, provide:

- Passwords containing characters belonging to 3 of the 4 following categories: uppercase characters (A - Z), lowercase characters (a - z), base digits 10 (0 - 9), non - alphabetic characters (for example!, $, #, Or%);
- Not equality with the user profile;
- Passwords not easily attributable to the operator;
- Password known ONLY to the operator, chosen by the latter at the first access to the system.

Some indications are given to help in choosing passwords that can be considered safe:

Safe passwords

Passwords with a satisfactory level of security must have the following characteristic:

- They are composed of uppercase and lowercase characters.
- They also use punctuation characters, such as; [,], * ", and a combination of numbers and letters.
- They must not represent a word in any language or dialect that is sufficiently widespread.
- They must not be based on personal information, such as names of family members, dates of birth, anagrams, or combination of names and similar.
- Another important precaution is the selection of key words, which can be easily typed on the keyboard, without having to look at it, to minimize typing time and to prevent typing surreptitiously from third parties nearby.

Weak passwords

It is emphasized that the passwords that are easy to identify have the following characteristics:

- The password can be found in a common Italian dictionary, in English or other common language.
- The password is a commonly used word, such as the name of some family member, pets, friends, collaborators or fictional characters.

- The password related to computer expressions, hardware and software, as well as those related to dates of birth or other personal information, such as address, telephone number and similar.
- The numerical sequences of the type aaaaaaaa, bbbb, 121212, 123456, etc. Word as listed above are to be discarded, typed in reverse.
- Any of the passwords previously indicated as weak, preceded or followed by a figure such as for example giovanni1, or 1giovanni.

Recommendations for the protection of the password

- Do not use the same password for internal authentication systems and for external authentication systems, such as access to your bank account and other activities, not related to the institutional activity of the Company.
- Do not share the password with any subject, internal or external to the Company, including superiors, at any level.

All the passwords that have been generated by the person authorized to process personal data must be treated as strictly confidential.

In particular, here is a list of the measures to be taken:

- Do not disclose passwords through the phone to anyone.
- Do not write the password on any document and do not hide it in any part of the office.
- Do not store the password in any type of computing system, including a mobile phone, a handheld computer, and similar.
- Do not write a password in an e-mail message.
- Do not talk about passwords in front of third parties.
- Do not give any indication as to the format and the length of the password in use.
- Do not disclose the password to work colleagues while on vacation;
- Never use the feature, offered by several applications, to memorize the password.

In the case of system operations that require your password (eg: change of the PC or installation of programs), the system operators or persons appointed by the Data Controller will change it temporarily, giving you communication. When using the PC for the first time, it is mandatory that you change the password immediately.

If someone insists to know your password, first refer to this document and then immediately inform your contact person.

If you have even the slightest suspicion that your password has been compromised in some way or become known by third parties, immediately replace the password and report the incident to your reference manager.

If the person authorized to process personal data has any doubts concerning the safe methods of generating, using and keeping the passwords, he must contact the information systems manager as soon as possible to obtain appropriate clarifications and instructions.

4.2 UNATTENDED PROCESSING SESSIONS

It is recommended not to leave the electronic instrument unattended and accessible during a session of personal data processing, in particular, whether it is necessary to move away from the workplace temporarily, by pressing the Ctrl + Alt + Del keys at the same time it is possible to activate the Windows Protection "from which you can press the "Lock Computer" button to lock the workstation without having to exit the programs you are using. Once you are back in front of your workstation, to resume operation you must follow the instructions on the windows video by pressing the Ctrl + Alt + Del keys again and entering your password.

Remember that, for greater security, a screen saver can be configured on each workstation with an unlock password that takes action after n. minutes of inactivity.

4.3 RECOMMENDATIONS FOR SAVING DATA IN THE NETWORK

Please note that the only areas authorized for saving personal data processed with Office Automation tools (word, excel, etc.) are the reserved spaces on the server. These spaces are configured in order to ensure the security and the custody of the data, guaranteeing their availability in case of emergency and subjected to backup in compliance with the legislative provisions on the matter.

In particular, personal data managed by each person authorized to process personal data can be saved in the following types of network folders:

- Personal folders in which each person authorized to process personal data saves his working documents.
- Folders shared by all the persons authorized to process personal data where data related to common projects and / or activities are stored.

Any local backup is strongly discouraged and is under the full responsibility of the person authorized to process personal data.

4.4 RECOMMENDATIONS FOR THE CUSTODY, USE AND DESTRUCTION OF REMOVABLE MEDIA

Generally, it is not recommended to copy personal data on removable media (CDs, USB sticks, etc.) in order to minimize the risk of loss or destruction of data, even if accidental.

Having said that, where in carrying out the normal activity assigned to the persons authorized to process personal data, in the context of his authorization profile, it is essential to make a copy of personal data on removable media, the following precautions have to be observed:

- Make sure that removable media is properly formatted and free of other files that may be infected. When in doubt, it is always a good idea to re-format the media before registering personal data.
- Mark the removable media with a label, showing the indication in clear text or in code, to allow the person to immediately recognize the content of the support in question, and to prevent it from confusing it with other media in its possession.

Removable media containing personal data have to be directly and personally guarded by the person making the copy.

If the data contained on removable media are no longer justified, it must be immediately formatted.

Since removable media are particularly sensitive to magnetic fields, to avoid erasure or even accidental data corruption, they must never be approached to a magnetic field, such as a speaker magnet, or left abandoned near a transformer, such as the transformers used in table lamps, in so far as the dispersed fields could damage their contents.

Be careful not to forget the removable media inside the computer when, at the end of the copy, the computer turns off and you go away.

The removable media containing personal data must never be left on the table, but it has to be immediately placed inside a safe case when not in use; depending on the relevance of the stored data, it can be placed in locked desk drawer to an armoured cabinet or a safe, suitable for storing magnetic supports.

4.5 RECOMMENDATIONS FOR THE USE OF HARDWARE AND SOFTWARE

The software installed in each machine as well as the related hardware configuration, reflect the necessary and sufficient condition for the usual work to be carried out.

If the person authorized to process personal data deems it necessary to have a new software or hardware update for the usual tasks, it is necessary to send a specific request to the Information Systems manager who will evaluate the question, in agreement with the responsible privacy manager.

It is good to remember that any software, except for those called freeware, has a license and the improper use of this can lead to civil consequences.

4.6 INTERNET AND E-MAIL

The use of internet and e-mail is made available by the Data Controller mainly for business purposes, ie in order to comply with the tasks provided for by their role. It must be remembered that the use of e-mail can entail risks deriving from the possible interception of the information exchanged and, therefore, the documents therein contained could be read and / or used by people that are unrelated to the correspondence.

When an e-mail is printed, it assumes all the characteristics of a paper document and the operator must follow the instructions regarding this type of processing.

The e-mail service is considered to be a working tool for all purposes, such as fax, telephone and therefore the employee has to make appropriate use of it, which does not fall outside the working context in which it operates; sending personal e-mails is not prohibited. However, this use must be bounded to a limited e-mail number or only during the break time.

With regard to Internet connectivity, it is forbidden to download large files (usually music files, movies, video ...) as this operation involves the saturation of the band, slowing down those who use the Internet for consultation for business purposes. It is also forbidden to download executable programs from the Network unless previously authorized by the information systems manager.

(insert company name) considers Internet as a useful and profitable tool when used in the professional environment in which the operator works. If abuses emerge in the use of it by an operator, the access for him is denied.

5. NON-AUTOMATED PROCESSINGS

5.1 DAILY MANAGEMENT OF PAPERWORK

General instructions for personal data

- Paperwork containing personal data should normally be placed in closed archives. A locked room is also considered as closed archive.
- The paperwork are taken by the persons authorized to process personal data, only to the extent and for the time strictly necessary for the performance of the related tasks, at the end of which - and in any case at the end of the working day / week - are placed in the archives. Each operator must take care to verify that the paperwork entrusted to him do not remain unattended, especially in contexts where data are accessible to subjects not in charge of processing (transit areas, waiting rooms, meeting rooms, and so on).

- Even during the working day, in case of removal from the workstation for a significant period of time, the files are stored in the archives, with the exception of appropriate guarantee of control by other operators in charge of the same processing. In any case, the paperwork should never be left unattended on the table during the day.
- The loss or theft of information must be immediately communicated to your reference manager.
- It is a good rule to avoid excessive proliferation of prints and photocopies of documents containing personal data. The scanned prints and photocopies must be destroyed in the appropriate paper shredder, if available, or they must be torn in small pieces.

Instructions for special categories of data

In addition to what is required for personal data in general, paperwork containing special categories of data, such as data concerning health or judicial data, are stored in controlled access archives and are controlled and kept by the operator until the restitution, so that it is impossible for persons without authorization to access (including other data processors who are not authorized to access to special categories of data), and are returned at the end of the operations entrusted.

5.2 KEYS MANAGEMENT

The persons in charge of the management of the "physical" keys of the archives have to:

- Check the correct functioning of the keys in the moment that they are handed over;
- verify that the keys do not remain inserted in the reference cabinets / archives;
- keep the keys in a place and in ways that ensure the appropriate level of security even to the type of archive;
- not make the keys available nor, if possible, show them to strangers;
- in case of loss or theft, immediately report it to the Contact Person and request the prompt replacement of the lock, moving the documents from the unprotected archive if necessary for the required time.

5.3 ARCHIVE WASTE

The archive waste, that is the periodical disposal of paper material containing personal data, must be carried out avoiding that personal information, especially if belonging to special categories, can be used by not authorized subjects.

In particular, special categories of data must be disposed of, using the appropriate tools for the destruction of documents, where available, or, in the absence of the latter, the sheets containing special categories of data must be torn in small pieces before being trashed.

5.4 FAX USE

If you need to send a fax containing personal data to a person authorized to view them, you must ensure that the recipient is close to the fax at the time of shipment / receipt. If the fax is sent outside the working hours, the fax machine must be placed in a closed room and accessible only by the persons authorized of processing the transmitted data.

5.5 CALLS AND TALKS

It is strongly recommended never to speak loudly when processing personal data by phone, especially using mobile phones outside the Company or even inside, in the presence of unauthorized third parties, in order to prevent personal data from being disclosed to unauthorized third parties, even accidentally.