*Translation from Italian into English*

**Data Protection and Security Regulation**

FOGLIANI Spa – FUTURTEC Srl

FOGLIANI ROMANIA

**DOCUMENT CHECK**

|  |  |  |  |
| --- | --- | --- | --- |
| DOCUMENT CODE | REVISION LEVEL  1.0 | ISSUING DATE  March 07, 2019 | TYPE OF DOCUMENT  POLICY |

***Table of Contents***

[1 INTRODUCTION 3](#_Toc6243133)

[1.1 PURPOSE 3](#_Toc6243134)

[1.2 RECIPIENTS 3](#_Toc6243135)

[1.3 REVISION AND UPDATING THE DOCUMENT 3](#_Toc6243136)

[2 LEGISLATIVE REFERENCES 4](#_Toc6243137)

[2.1 REGULATIONS ON THE PROTECTION OF PERSONAL DATA (EUROPEAN REGULATION 2016/679) 4](#_Toc6243138)

[2.2 CHANGES AND ADDITIONS TO THE RULES OF THE CRIMINAL CODE AND OF THE CRIMINAL PROCEDURE CODE ON THE SUBJECT OF COMPUTER CRIME, LAW NO 547 OF 1993 6](#_Toc6243139)

[2.3 REGULATION OF COPYRIGHT (LAW 633/41) 6](#_Toc6243140)

[2.4 ADMINISTRATIVE LIABILITY OF CORPORATE ENTITIES (LEGISLATIVE DECREE 231/2001) 7](#_Toc6243141)

[2.5 FAILURE TO COMPLY WITH THESE RULES OF CONDUCT. 7](#_Toc6243142)

[3 ACCEPTABLE USE POLICY 8](#_Toc6243143)

[3.1 GENERAL DATA SECURITY POLICIES 8](#_Toc6243144)

[4 SPECIFIC RULES 11](#_Toc6243145)

[4.1 PHYSICAL AND LOGICAL ACCESS 11](#_Toc6243146)

[4.2 INSTRUMENT SAFETY 12](#_Toc6243147)

[4.3 DATA STORAGE AND AVAILABILITY 15](#_Toc6243148)

[4.4 MANAGEMENT OF PAPER DATA 16](#_Toc6243149)

[5 PASSWORD POLICY – USER ACCESSES 17](#_Toc6243150)

[5.1 AUTHENTICATION 17](#_Toc6243151)

[5.2 EMAIL POLICY 20](#_Toc6243152)

[6 INTERNET POLICY 22](#_Toc6243153)

[7 VERIFICATIONS AND CHECKS 23](#_Toc6243154)

[7.1 PROCEDURES FOR VERIFICATION 23](#_Toc6243155)

[7.2 INFORMATIVE ACCORDING TO ARTICLE 13 OF EU REGULATION 23](#_Toc6243156)

[7.3 PENALTIES 24](#_Toc6243157)

# INTRODUCTION

This document represents the regulation of Fogliani and associates/subsidiaries on the privacy and security of personal data.

For Fogliani information security is a necessary condition in order to achieve institutional goals: safeguarding company data and related information systems allows Fogliani to provide quality services ensuring the reliability of the service offered.

Through the corporate information systems, numerous personal data are processed in relation to which the Italian and European regulations on privacy require the implementation of technical and organizational security measures and the active involvement of the parties in charge of such processing, in order to guarantee an adequate protection of such data.

The protection of company data basically depends on the compliance of rules of conduct that allow to preserve the Confidentiality, Integrity and Availability of such data over time (RID criterion).

## PURPOSE

Since this is a policy and not a procedure, there are no specific activities and flows of operations.

The primary objective of this policy is to ensure that all users adapt their conduct according to the detailed instructions below.

This will contribute to achieving the safety objectives, which can be summarized in three distinct aspects:

* **Confidentiality**, i.e. ensuring the prevention of unauthorized or abusive access to information, services and systems;
* **Integrity**, i.e. ensuring that the information has not been altered by accident or abuse.
* **Availability**, i.e. ensuring access to information and network services by the personnel in charge in relation to business needs;

## RECIPIENTS

This document is intended for all employees and internal collaborators of FOGLIANI Spa, FUTURTEC Srl, FOGLIANI ROMANIA Srl

## REVISION AND UPDATING OF THE DOCUMENT

The revision and updating of this document are the responsibility of the Executive Management and the IT function, which make use of the support of all the other corporate structures in relation to the areas of expertise.

# LEGISLATIVE REFERENCES

In the last few years, Italian legislation has established a set of rules aimed at guiding companies in achieving a balance between what technologies can achieve and the need to protect data that often does not belong to the individual subjects that manage them.

Complying with the information security rules, means avoiding the legal risk or incurring criminal/administrative penalties following the failure to comply with laws or regulations.

With regard to data security in the company, it is possible to summarize the Italian and European reference legislation in the following items:

* Regulation (EU) 2016/679 of the European Parliament and of the Council concerning the protection of individuals with regard to the processing of personal data of April 27, 2016
* Code regarding the protection of personal data (Legislative Decree 196 of June 30, 2003), partially repealed and amended by Decree 101/2018
* Provision of the Privacy Guarantor
* Changes and additions to the rules of the Criminal Code and of the Criminal Procedure Code on the subject of computer crime, Law No 547 of 1993
* Copyright law (Law 633/41)
* Legislative Decree 231 of June 08, 2001 on the Administrative Liability of Corporate Entities

## Regulations on personal data protection (European Regulation 2016/679)

The **General Data Protection Regulation (GDPR)**, or the EU Regulation No 679/2016 on the protection of personal data (or Privacy Regulation), came into force May 24, 2016, and becomes fully applicable from May 25, 2018, repealing Directive 95/46/EC from which the various national regulations (including the Italian Text on Privacy - Legislative Decree 196/2003) have arisen.

The Regulation relates to the protection of individuals with regard to the processing of personal data, as well as to the free circulation of such data, which are to be understood as “any information concerning an identified or identifiable natural person”.

It is no longer a purely legal norm, but there is also an economic impact because the legislator wanted to introduce the rules necessary to bring order to the digital economy, dominated by the giants of the web.

**General principles**

As basically already established by Legislative Decree 196/2003, the Regulation guarantees that *“the protection of individuals with regard to the processing of personal data is a fundamental right”*.

The legislator proposes to standardize the application of the protection of personal data within the Union, to ensure a consistent and high level of protection of the fundamental rights and freedoms of natural persons, and to remove obstacles to the circulation of personal data to within the Union.

Any processing of personal data should be lawful and correct. The ways with which personal data concerning them are collected, used, consulted or processed should be transparent to natural persons, as well as the extent to which personal data are or will be processed.

The principle of transparency requires that information and communications relating to the processing of such personal data be easily accessible and understandable and that simple and clear language is used

The European Regulation provides among its pillars the principle of **Accountability** (which could be translated into “accountability and reporting requirement”) which concerns all subjects.

The Owner of data processing shall be able to demonstrate that he has adopted an overall process of legal, organizational and technical measures for the protection of personal data, also through the development of specific organizational models: he shall demonstrate in a positive and proactive way that the data processing carried out is adequate and compliant.

**News from Europe**

In addition to the aforementioned and fundamental principle of Accountability, with the European Regulation some interesting innovations have been introduced to protect personal data:

* The **“Privacy Impact Assessment”** (preventive assessments of impact on data protection) in the case of risky processing; that is to say, a precise risk analysis is mandatory. The text of the Regulation specifically mentions the parameters of gravity and probability of the event
* The appointment of a **“Data Protection Officer”** (responsible for the protection of personal data), who shall be competent, independent and not necessarily internal to the entity/company. The appointment is mandatory in some cases (e.g. personal data at risk) but all organizations have the right to appoint him for a correct and effective management of a privacy system
* The figures of the **“joint controllers”** (Co-owners), who may divide or share the privacy liabilities in a specific contract, which shall be taken into account in the event of controls or disputes. This innovation could be useful, especially, in the cloud computing sector (until today difficult to classify in the old schemes owner/responsible).
* The concept of “main establishment” of the owner, in order to prevent a company operating in several EU countries from facing the national requirements of each individual State.
* The role of “Lead Authority”, to ensure that there is only one Guarantor each time responsible for the procedures with multi-State impacts
* **Penalties** much heavier than in the past: up to 4% of a company's total business turnover. The purpose is clearly to make data protection a sensitive issue also and above all for large multinationals (for example Google, Facebook, Microsoft)
* The obligation to comply, in the conception of new products or services, with the principles **“Data Protection by Design”** and **“Data Protection by Default”**, i.e. the application of data protection right from the design stage of any processing
* The right to be forgotten, for which any interested party can request the removal of their personal data for legitimate reasons (for example, we can ask to be “forgotten” online).
* The ***Data Breach***, i.e. the notification of a violation to the authority, if possible within 72 hours, and the communication to the interested parties.

**Impact on the security of processing**

At the Community level the discipline on the subject of data processing security is maintained in its general structure; however, greater attention is being paid to the so-called *risk-based approach* and some of the main types of technical and organizational measures are specified in a more descriptive and illustrative way.

Furthermore, the detection of the effectiveness of the security measures adopted (Article 32, letter d) and above all the impact assessment (known as *DPIA - Data Protection Impact Assessment*) as a fundamental instrument to know the current status and the margin of improvement of your privacy system.

In general, is reiterated one of the fundamental concepts of information security: guaranteeing confidentiality, integrity and availability (known by the acronym RID).

How to keep track of all this? The EU Regulation provides for the owners or data responsible of the processing the obligation to adopt and maintain documentation similar to the Security Planning Document provided for by Legislative Decree 196/2003.

For example, there is an obligation to keep a record of personal data processing activities, including a general description of the technical and organizational security measures adopted. Formally, small companies that do not have risky processing can be exempted from this obligation; however, it is advisable to adopt this register, which allows in any situation to clearly demonstrate the type of personal data managed.

Summing up, the owners and data responsible of the processing are required to adopt organizational and technical security measures aimed at mitigating the risk according to a proactive approach (accountability), identifying the risks associated with the processing (so-called risk-based approach) and adopting appropriate measures that take into account the principles of transparency in addition to the principles of privacy by design (privacy from design) and by default.

## Changes and additions to the rules of the Criminal Code and of the Criminal Procedure Code on the subject of computer crime, Law No 547 of 1993

Law 547/93 introduced the concept of computer crime within the Regulations of the Criminal Code and the Criminal Procedure Code. In this regard, it has made it possible to prosecute computer crimes in a manner very similar to the traditional ones, providing for the offender to impose variable penalties up to a maximum of five years of imprisonment. The computer crimes considered and the Articles of the Criminal Code that have been replaced are listed below:

* Attack on computer systems of public utility (Article 420)
* Forging of electronic documents (Article 491 second)
* Unauthorized access to an information or electronic system (Article 615 third)
* Unauthorized possession and distribution of access codes to information or electronic systems (Article 615 fourth)
* Dissemination of programs aimed at damaging or interrupting an information system (Article 615 fifth)
* Violation of online correspondence (Articles 616-617 sixth)
* Email interception (Article 617 fourth)
* Damage to information and electronic systems (Article 635 second)
* Computer fraud (alteration of the integrity of data for the purpose of obtaining an unfair profit (Article 640 third)

The knowledge of the crimes listed above allows users to prevent any criminal conduct during the use of information instruments and to better understand the need to apply some of the rules described below.

## Regulation on copyright (Law 633/41)

The Law No 633 of April 22, 1941 which regulates the “Protection of copyright and other rights related to its exercising”, revised with the Law No 248 of August 18, 2000, and with the subsequent Legislative Decree No 68 of April 09, 2003, sets up criminal and administrative penalties for those who violate the copyright. According to this Regulation, in the event of ascertaining the illicit use of software products in the company, the legal representative and the eventual manager of the IT Department can be held responsible, if it is ascertained that the offence was carried out directly by the company, while the final user will be held responsible, if it is ascertained that the latter has introduced illegal copies into the working environment without the company being aware of or in contrast with the regulations in force in the company. The abusive use of software therefore involves two types of risks, one of a technical nature and one of a legal nature:

* Risks of a technical nature: the use of counterfeit programs within the corporate network can lead to the spread of viruses and the malfunctioning of the company's systems (loss of data and operations) due to incomplete and incompatible copies between them;
* Risks of a legal nature: in their capacity as works of intellect, software products are protected by the legal regime of copyright. Copying and using software products without having obtained the necessary authorization from the rights holder constitutes a crime. The legal risks to which this is exposed include civil and criminal penalties.

With regard to the abusive duplication of computer programs, instead, those who commit this crime risk criminal penalties to which can be added a pecuniary administrative penalty, or a fine that can reach twice the market price of illegally copied programs.

FOGLIANI provides its users with all the software instruments necessary for the performance of their work and guarantees their compliance with copyright law. It is therefore necessary for users to strictly adhere to the rules regarding the business software in order to avoid the risks associated with the introduction of unauthorized or harmful programs.

## Administrative Liability of Corporate Entities (Legislative Decree 231/2001)

Decree 231/2001 introduced into the Italian legal order the Administrative Liability of Corporate Entities for certain crimes and offences which, even if carried out physically by subjects in senior positions or employees of the entity, can be considered directly connected to the same if “committed in his interest or advantage”.

Types of crimes prosecuted by the Legislative Decree 231/2001:

* crimes against the public administration
* corporate crimes
* counterfeit currency crimes, public credit cards and revenue stamps
* crimes of insider trading and market abuse
* crimes with terrorist purposes

For the crimes provided for in the Decree, the entity is liable only if the commission of the crime was made possible by failure to comply with the obligations of management and supervision. The omission of these obligations is excluded if, before committing the crime, the entity has adopted and effectively implemented a model of organization, management and control, suitable to prevent crimes of the type from that which occurred.

## Failure to comply with these rules of conduct.

FOGLIANI reserves the right, within the limits of the law, to verify compliance with these standards for verification of the correct functioning of the systems.

FOGLIANI reserves the right to revoke the authorization to access Internet and email instruments in the event of failure to comply with the above listed standards.

It should also be noted that, based on specific legal provisions, both access to the company information system for purposes not permitted by the company and - once obtained access - to remain connected to the aforementioned system for purposes that are not equally permitted may constitute a criminal offence (Article 615 third of the Criminal Code) as well as constituting a breach of contractual obligations relevant to the disciplinary plan.

Furthermore, please note that the Criminal Code (Article 615 fourth) expressly hypothesizes imprisonment towards those who “in order to procure a profit for themselves or others or to cause damage to others, illegally procures, reproduces, disseminates, communicates or delivers codes, keywords or other means suitable for access to an information or electronic system, protected by security measures, or in any case provides indications or instructions suitable for the aforementioned purpose”.

# ACCEPTABLE USE POLICY

The security of the FOGLIANI information system is a fundamental requirement to guarantee the reliability of the processing information, as well as the effectiveness and efficiency of the services provided by the company. The security of the information system has as its primary objective the protection of data and elements through which the data is managed.

The protection of data and associated elements is guaranteed if it is preserved:

* **confidentiality:** ensures that data is accessible only to those who are authorized to have access to it;
* **integrity*: safeguards the completeness of data and transfer methods***;
* **availability:** ensures that authorized users have access to data and elements that process them when necessary;

The lack of an adequate level of data security, in terms of Confidentiality, Availability and Integrity, can have as consequence the loss of competitive advantage, image, customers, turnover and a consequent significant financial loss. To all this we shall also add the risk of incurring penalties related to violations of current regulations.

Therefore, the security of the information system is obtained by implementing a series of adequate security measures, i.e. procedures, technical mechanisms or practices that reduce the risks to which the information assets as a whole are exposed.

FOGLIANI directs its activity to compliance with current legislation, with particular reference to the Personal Data Protection Code, not only to avoid the risk of company involvement, but above all, to guarantee an adequate level of data security personal details of the company and its information system.

## General data security policies

This paragraph indicates the fundamental principles that inspire the FOGLIANI data security regulations.

### Company information systems

The company information system is composed of a set of central server units and client PCs connected to a local area network (LAN), which use different operating and application systems.

FOGLIANI provides its employees and internal collaborators with all the instruments necessary to perform the assigned tasks. The software instruments and applications provided by the company are work instruments and shall be used for these purposes. The data contained within the work instruments are considered company data and as such owned by the company. Accordingly, the company can fully dispose of them and users will not be able to have privacy expectations with respect to the information sent, received or stored.

It should also be remembered that improper use of company systems includes the processing, transmission, recovery, access, display, storage, printing and in general the dissemination of fraudulent, harassing, threatening and illegal materials and data, racist, of sexual orientation, obscene, intimidating, defamatory or in any case not congruent with professional conduct.

Therefore, no data of this kind shall be present on the FOGLIANI network, on Personal Computers, within applications (such as email, Intranet portals, etc.) and in personal or shared network folders.

Furthermore, users of corporate systems should not use the infrastructure to do business, sell products, or for any other business other than those expressly provided for by the company management.

**Access to information.**

### Access to information

Access to information by every single user shall be limited to the information he needs to perform his duties (*need to know* principle). The disclosure and transmission of information internally, as well as externally, shall be based on the same principle.

### Personnel and security

The company plans and carries out training and information activities for personnel, with particular attention to information security and the correct use of company instrumentation.

Personnel shall be required to guarantee a minimum level of security to the assigned equipment. Theft, damage or loss of work instruments shall be promptly reported.

Personnel (including consultants and external collaborators) shall sign confidentiality clauses which shall be reiterated at the time of termination of the employment relationship.

Failure to comply with what is indicated in this document and in all the others that arise from it constitutes “carelessness of the company property” and will therefore be subject to disciplinary sanctions according to when indicated by Article 7 of Law 300/70 and by the National Collective Employment Agreement.

### Accidents and deficiencies

All employees are required to detect and notify IT personnel of any issues related to corporate security.

### Physical Security

Access to buildings and relevant premises for the protection of property and data shall take place only after identification of the authorized subjects. The identification and design of physical security countermeasures shall take into account both the possibility of the materialization of physical threats and regulation and legislation in force.

Apparatus maintenance shall be performed in accordance with the manufacturer's instructions or with documented procedures to ensure service availability and integrity.

### Information Security

The design and implementation of the IT security plan shall take into account both the possibility of materializing internal and external unauthorized access attempts, and regulation and legislation in force and other constraints linked to company processes, industry certifications and regulations.

Users shall not exploit any weaknesses or failures of the information security system to damage systems or data, obtain resources for which they are not authorized, steal resources from other users or have access to systems for which they do not have the necessary authorizations.

### Verifications

Information systems shall be periodically controlled as well as the application of operating procedures.

The principles expressed in the general safety policies are specifically applied within the general safety rules and in those specific to the data processing, illustrated in the following chapters.

The personnel in charge of the IT function has been authorized to carry out interventions in the company information system, aimed at guaranteeing the security and safeguarding of the system itself, as well as for further technical and/or maintenance reasons (e.g. updating/replacement/implementation of programs, hardware maintenance etc.).

Such interventions, in consideration of the subsequently detailed rules on the use of email and Internet, may also entail access at any time, to the processing data by every single one, including email archives, as well as to verification on the websites accessed by the users enabled for external browsing.

Same right, always for the purposes of security system and to guarantee the normal operation of the company, is also applied in the event of prolonged absence or user impediment.

The IT personnel in charge has the right to remotely connect and view the desktop of every single PC workstations in order to guarantee technical assistance and normal operating activities as well as maximum security against viruses, spyware, malware, etc.

The intervention is carried out exclusively on the user's request or, in the case of objective necessity, following the technical detection of problems in the information and electronic system. In the latter case, provided that the necessary timeliness and effectiveness of the intervention are not compromised, the need for the intervention itself will be communicated.

# SPECIFIC RULES

## Physical and logical access

### Access to headquarters

Access to headquarters is allowed after identification of internal collaborators and visitors. It is necessary that the internal representative of the visitor always accompanies him during his stay in the FOGLIANI headquarters.

### Access to utility rooms and Data Centers

Access to these premises is restricted to authorized personnel only. In case of technical maintenance in the Data Centers, external personnel must be accompanied by an internal FOGLIANI representative.

### Management of physical access credentials to headquarters, premises and archives

These access credentials are assigned by the Management and/or by functions specifically delegated in relation to the access rights of the personnel. The delivery is recorded so that you always know the qualifications of every single employee or internal collaborator and in order to manage the possible return of the same (for example in the case of physical keys) once the relative authorization has been completed.

The existence of the conditions relating to access rights is periodically verified.

### Management of credentials for access to information systems

These access credentials are assigned by IT officers upon request of every single company divisions and Personnel Department. Each user accesses information systems with rights defined in relation to the job performed (e.g. use of specific resources such as applications and network folders). These rights are reviewed on the occasion of a change of job or termination of the employment relationship.

In order to keep users' authorization profiles up to date, the Personnel Department is responsible for communicating any organizational change to IT functions.

If a user should no longer be used, the IT operators start the termination procedure which includes the deactivation of the user, in order to avoid re-assigning this user to different subjects. In the event of disuse for a period exceeding 6 months, the access credentials are automatically disabled where the information system allows it or manually by the IT personnel.

When long-term disuse is known in advance (for example in the event of a long-term accident or maternity), it will be the responsibility of the Personnel Department to make specific communication to IT.

### Corrective and preventive maintenance of the systems

Systems shall always be updated to prevent vulnerabilities.

To this end, IT functions monitor the status of known vulnerabilities and updates to be installed, updating when possible, automatically or manually updates, or notifying users what activities to undertake to keep the systems always aligned and efficient.

### Suppliers

If FOGLIANI uses external companies for the management of information security and/or system maintenance, these subjects will be formally authorized and appointed and will assume the role, if applicable, of System Administrator or External Data Processor.

### Use of systems by third parties

External agents/consultants/sellers who, for the duration of the working relationship, shall access the company systems, are formally authorized by the Responsible of the area of expertise. The IT operators deal with the preparation of credentials and the profile of access to the systems based on the role that the consultant will have to fill and following the indications of the Personnel Office and/or the internal Responsible previously mentioned.

In addition to the contractual documents, all the external subjects authorized to access the company network must receive and sign the present data-processing rules.

Furthermore, if an external party uses its own PC to connect to the company Guest network, it shall guarantee that it has the most up-to-date version of the antivirus software and a communications protection system (e.g. VPN) installed, whenever it connect to its own company network or otherwise an external application.

PCs not owned by FOGLIANI cannot connect to company network resources, either via cable or WiFi.

Persons who are not employees, temporary collaborators, consultants or agents shall not be aware of and/or possess user-ID of internal users and, in the same way, shall not take advantage of the privileges granted by the company system, except for specific situations, authorized, related to maintenance activities of management applications or other information systems.

## Security of instruments

### Workstation protection

* Users shall avoid leaving workstations unattended with the work session open and active (login done) or with screens containing confidential data.
* Each user must enter the system lock (with CTRL-ALT-DEL + Block) when he leaves the workstation; the reactivation is regulated by password (equal to that of access to the company system).
* In addition, each user shall ensure that the workstation is protected by the screen saver or system lock that automatically starts after a defined time of inactivity (10-15 minutes); it is not allowed to modify this configuration or deactivate it. This type of measures serves to prevent the workstation (and therefore the open applications) from being used by others in its own absence
* At the end of the working day, all applications shall be closed according to the rules provided by the application itself. Improper closing may result in data loss or access by unauthorized persons.
* Turn off the PC at the end of the day (except for specific instructions from IT for maintenance activities) or in the case of prolonged absences, because leaving a computer unattended and connected to the network may be the cause of use by third parties without the possibility to subsequently prove its illegal use

### Proper use of electronic instruments

* It is forbidden to install programs originating outside that have not been expressly authorized by IT
* The use of programs for which the company has not acquired a suitable license is not allowed
* The use of electronic company instruments to duplicate and/or disclose material protected by copyright or patents is not allowed
* Changing the configurations set on your computer is not allowed
* The installation and use of software and/or hardware instruments to intercept, forge, alter or suppress the contents of communications and/or electronic documents are not allowed
* The installation on your computer of means of communication other than those made available by the company is not allowed.
* Avoid leaving unattended removable media (CDs, DVDs, tapes, USB sticks) containing company data on desks or in other places where they could be easily removed by unauthorized third parties. All the supports, and everything that is easily copyable, removable and concealable, when not used, must be placed in cabinets, shelves or drawers that are locked.

### More attention to laptops and other “Mobile” instruments

* The laptop, tablet and cell phone can be given in use by the organization to those in charge who during travel need to have electronic archives, automation support and/or connection to the organization's network.
* Due to the vulnerability of the information contained on mobile devices, particular attention should be paid to these types of systems and to limit as much as possible the uses at risk.
* Never leave the device unattended; if you are at other companies, you can use protection systems such as laptop security cables.
* Always keep the instruments with you when travelling. Never leave your laptop in your car, even if it is stored in the trunk, or in a hotel room, in the hotel lobby and in the waiting rooms of railway and airport stations.
* If a secure connection to the company system is not possible, perform a daily backup of any confidential data present on the portable device using external devices such as USB keys that IT personnel can make available (upon request).
* In the event of theft or loss, make a complaint to the relevant authorities and promptly notify the company (Personnel Office and IT functions) that will carry out, if necessary, what is necessary in order to prevent unlawful use of the users configured on the device

### Use of personal cell phone/smartphone

During working hours, including any breaks, those in charge are allowed to.

In the event of business trips away from the office, the personal phone can remain switched on, also to facilitate communication with the company where necessary.

In this case, however, we invite you not to use it for personal purposes, particularly in the presence of customers or suppliers.

Those in charge who are not employees (consultants, agents, external collaborators), can use their cell phones/smartphones to store company data only if expressly authorized and formally and personally taking on the entire responsibility for the processing.

These cell phones/smartphones must be evaluated in advance by the Data Controller, to verify the existence of adequate security measures.

### Attention to communication systems!

Network communications travel more and more often by means different than email: instant messaging software, social networks and other systems.

Remember that often these instruments are not able to protect the communications they carry.

For example, it is very simple to fill the shoes of another user with a full name; often the non-use of the HTTPS protocol facilitates malware attacks or the absence of advanced technologies for the encryption of communications allows the identification of sentences with extraordinary accuracy.

It is therefore not recommended to transmit company documents through this type of system, unless they are applications verified and authorized by the company.

### Antivirus

The presence of antivirus software is an essential security measure and a useful protection instrument. Its effectiveness depends in a fundamental way on the update which, as far as the users' computers are concerned, takes place automatically during the working activity.

Holders of laptops shall ensure that the antivirus is always up to date, for this purpose it is sufficient to connect frequently to the company network or to the manufacturer's site, making use of this way of the automatic update service. Detailed instructions are available through IT.

Given the considerable complexity reached by viruses, users do not have to try to eliminate them without the help of an expert. The antivirus system is automatically set to delete the viruses found.

If a more complex situation is suspected or the virus is quarantined because it cannot be deleted, the user shall immediately disconnect the computer from the network, turn it off and contact the IT operators.

This conduct will help to contain the damage caused to files and software and at the same time, ensures that the information needed to detect a new infection is recorded.

### Return of the instruments

Following the termination of the employment or consultancy relationship with the company or in any case when the validity of the assumptions for the use of the assigned instruments expires, at the discretion of the organization, the appointees have the following obligations:

1. Proceed immediately to return the devices in use;
2. Absolute prohibition of formatting or altering or tampering with or destroying the assigned devices or rendering the data contained in them unintelligible by any manual or automated process.

## Storage and data availability

* Necessary data for the performance of persona work activity (documents, images related to the business, email) shall be saved on the network resources made available by the company, in order to allow automatic centralized backup. Those in charge who work outside the company and who do not have the possibility of using network resources, must request the IT function to assign an external memory if they need to backup data on the local PC (more details below).
* It is recommended to:
  + save the data in the most suitable network folder according to the type of document and the methods used by the work group of which the user is part
  + do not preserve many versions of the same document on the network and, above all, once the same is consolidated, delete the previous versions, so that it won't needlessly occupy disk resources
  + avoid moving or deleting unused or unknown documents from folders; in any case, promptly notify the IT in the event of incorrect operations or failures
* Users shall not store on the network, in the common folders and on the company PC, assigned files and documents of a personal nature or that are not relevant to the professional activity, both to protect the privacy of each individual and not to needlessly occupy disk resources.

**Therefore, any file that is not related to work activity (e.g. personal photos, music files, videos) CANNOT be saved on company resources (network disks, shared storage, user PCs), even for short periods. The company reserves the right to immediately proceed with the removal of any file or application that it deems to be dangerous for the security of its systems or if it appears that these applications have been acquired or installed in violation of these Regulations.**

* The storage or dissemination of computer documents of an outrageous and/or discriminatory nature by sex, religion, race, ethnic origin, opinion and trade union and/or political affiliation is not allowed.
* Archiving of the company documents in cloud services NOT authorized by the IT function (e.g. Apple iCloud, Dropbox, personal Google Drive, personal One Drive, etc.) is not allowed
* Those in charge who work outside the company and who do not have the possibility of using network resources, shall request the IT function to assign an external memory (USB key, external hard drive, memory card) on which to temporarily copy of the data or, to be used to backup the data present locally on the laptop or fixed PC. The IT function will evaluate the user's needs and eventually assign the type of equipment that it deems most suitable. The user shall follow the instructions provided by the IT for the use of the memory and in particular for backup operations. These devices shall also be kept with diligence both during travel and use in the workplace; they shall be used exclusively by the persons to whom they have been assigned and, under no circumstances, shall they be handed over to third parties. Any loss of data related to the failure to perform the backup will be the responsibility of the user to whom the device was assigned.

## Management of paper data

### Correct management of paper documents

Those in charge of processing, which have been entrusted with documents containing personal data, shall preserve these documents with the necessary precautions and store them (including any copies) at the terminal of the processing operations.

It is recommended to:

* Verify the functioning of the locks through the key of the cabinets and containers containing sensitive data or however confidential nature (also for the temporary preservation of documents)
* Assign the keys of the cabinets/containers to the authorized personnel only, who shall store them with care
* Do not leave documents inside printers, photocopiers or fax machines
* Do not leave documents visible on the desk (*clean desk policy*) when you leave the room or receive someone for a meeting
* If you have a personal office, lock the room when you leave for breaks, meetings, commitments outside the company; otherwise close the archives, drawer units, etc.

### Particularly confidential documents

**Paper documents containing sensitive, judicial or important personal data shall be protected and their circulation must be restricted.**

Users authorized to manage paper documents containing personal data of particular categories (*formerly sensitive data*), judicial or deemed important, shall ensure that these documents cannot be viewed by unauthorized subjects even during work activity, taking care not to leave such documents unattended documents near printers, photocopiers or fax machines and store them in locked cabinets. The circulation of this documentation must be restricted to authorized personnel only.

### Practical advice

A few examples and practical suggestions for users of all headquarters. Particular attention should be paid to those who work in the Branches, where the rooms are smaller and used in a shared way for different needs.

* Use the meeting room, where present, to receive customers and suppliers
* If you need to receive people outside your desk to use the PC, make sure you do not leave confidential documents in sight (offers, price lists, contracts, tender specifications, etc.)
* Generally, store the business practices in cabinets, drawer units, archives at the end of work
* Attention to personal data recorded on the packages (phone numbers, etc.); enter only the information needed to manage the delivery
* Documents with contact lists, e-mailings, etc. must not be left on sales counters.
* Preserve any proposals, specifications, documents left by installers for the preparation of a project and budget with the necessary confidentiality

# PASSWORD POLICY – USER ACCESSES

## Authentication

### Access credentials composition.

Each user, to access the company computer systems must be previously identified and authenticated, by verifying their credentials. The credentials consist of:

* user’s unique identifier (user-id)
* secret keyword (password).

The credentials are confidential and strictly personal and are assigned to each employee who shall use a workstation, connected to the company IT network, as a work instrument. The key words (password) form “security measures” prepared in compliance with specific legal obligations. For this reason communication to anyone and in whatever capacity is prohibited; there are no exceptions to this provision, even with regard to one's direct supervisors. The prohibition refers to any possible form of communication of authentication credentials, both oral and written (phone, e-mail, etc.).

Please note that the use of the company information system and consequently access to data, programs and corporate IT resources is permitted in order to allow the performance of duties and/or assigned tasks for the time required to perform these duties and tasks.

### Keyword composition rules

Within the deadline of your keyword, in some cases automatically reported, each user will have to update, according to the methods in use, the same keyword respecting the following rules:

* adopt a combination of numbers and letters (alphanumeric) with a length of at least 8 characters; we also recommend the combined use of upper and lower case and a special character
* should not be based on personal information (name of family members, car registration number, date of birth, part of your name/surname, geographical location, etc.)
* do not use an acronym, a common saying, a dialect word or slang
* it shall not be a common sequence of characters such as 123456, aaabbb, qwerty, etc.
* it shall not be based on easily identifiable company terminologies such as the company name and its derivations or product codes/names

Generally, the password shall be sufficiently complex in terms of combination of characters but it should be easily remembered by the user.

A possible technique is to use sequences of characters without obvious meaning, but with single characters that form a sentence that is easy to memorize, such as a movie, book or song title. e.g.: I7N0m3de88aR%sa = The Name of the Rose.

### Confidentiality of the keyword

All users shall ensure maximum confidentiality of the keyword; all access passwords shall be treated as sensitive and confidential company information, and therefore the following indications shall be respected:

* do not communicate it to anyone else;
* do not disclose passwords in e-mail messages or other electronic forms of communication
* do not disclose your password to anyone on the phone
* avoid keeping a written record;
* type it always being careful not to be observed by anyone;
* immediately update it in the event of a breach of confidentiality, even if only suspected

### Updating the keyword.

It is necessary to update the keyword in the following cases:

* to the first connection into the IT system (e.g. network and company servers, applications) for replacing the assigned “initial” keyword, which is usually temporary;
* when reported automatically by the system (or at least every 90 days if managed manually by the user);
* every time you suspect or believe that the keyword has lost the confidentiality requirements

Please note that, when carrying out the update operation of the keyword, the new one must be composed in compliance with the rules previously defined.

The keyword shall be updated on all operating systems or applications that require the use of credentials, regardless of the presence of an automatic expiration system.

### Deactivation of user credentials

The credentials for accessing the domain or applications will be deactivated in case of non-use of the same for a period exceeding six months. If the non-use is linked to known absences (for maternity or long injury), the Personnel Office will inform the IT division.

The user will then have to request, in the manner currently in force, the reactivation of his credentials to the IT division.

### Disabling a user's authorization

Authorizations to access the computer system are disabled in the event that the user no longer needs to access certain information or services in order to guarantee the correspondence between the organizational duty performed and the access rights to the data.

### Access to data in case of need

In case of need (for example sudden and prolonged absence), it is expected that the user's keywords will be reset and replaced to allow access to the data by an authorized organizational figure. This need is communicated to the user who is the holder of the access credentials, who shall then provide, according to the methods currently in force, to update them.

### Management of the termination of the employment relationship

The Personnel Office shall communicate all significant changes in user assignments and/or employment status to IT functions, so that the operators in charge can carry out the necessary operations on users.

Following the termination of the employment relationship, we proceed with the following activities:

* the user-id is disabled from Company Information Systems
* the email Inbox (if nominative) is deactivated and its contents deleted at the latest within fifteen days from the end of the employment relationship; it will therefore be appropriate to carry out the necessary handovers and communications outside the company (if applicable) with the references of the new partners
* if the leaving user used a functional/generic email Inbox, this Inbox will be made available to the new appointee
* the content of the work tools can be evaluated by the user supervisor, who decides in a short time if it should be reused and then reassigned or cancelled, communicating the choice to all qualified offices

It is recommended that the user leaving the company not to delete company-owned data from the personal computer, while any personal data (of a non-working nature) shall not be present on the company equipment that shall be returned.

### Security checks

As part of the activities concerning the protection of the security of the technological infrastructure, the company could carry out periodic analyses on user passwords in order to verify its solidity, management policies and duration, informing the users in advance.

In the event that the audit has, among the possible outcomes, the decoding of the password, it will be blocked and the assignee is asked to replace it with a more secure one.

## EMAIL POLICY

### Email - General Rules

* Email is a communication mean owned by the company, assigned to the person in charge to carry out his tasks.
* Generally, an email message sent by a qualified email address by [name.surname@companyname](mailto:name.surname@companyname) or function@companyname is sensed as containing information, news, opinions of an official nature coming from the company. Consequently the use of electronic mail shall be considered equal to the use of company headed paper.
* Each is responsible for the content of their communications, including with regard to the confidentiality of the data processed within: improper disclosure could be considered a violation of company secrecy or a violation of current regulations.
* Personal use of the company email Inbox is not allowed. Any information of a personal nature shall not pass through the company's mail servers, which may be subject to checks during maintenance activities or in the event of anomalies, breakdowns or safety-related interventions; users will therefore not be able to have privacy expectations with respect to the information sent, received or stored. In case of receiving personal mail on the company email Inbox, the user shall immediately cancel each message.
* It should be remembered that the company provides “functional” email addresses shared by several workers, alongside individual ones. It is recommended to use it to manage all those communications that shall be shared within the work group.

### Email - Security

* + The configuration on the company computer of your personal email account (e.g. on your Outlook client, Mozilla, etc.,) is not authorized. Instead, you can consult your personal email Inbox through Webmail applications (e.g. Gmail, Yahoo, Libero, Fastweb, etc.) while respecting the methods of use of the network defined in this procedure. It is also allowed to access your email account through the company smartphone (or similar device), always within the limits of a minimum commitment that does not impact on the work activity and on its own efficiency and productivity. Please note that the personal email SHOULD NEVER be used to process company data.
  + The company has adopted numerous email protection systems against viruses and spam activity. However, we take this opportunity to reaffirm some fundamental rules for the email correct use:
  1. Users shall not open email attachments of which the sender is not known with certainty or about the safety of which even the slightest doubts arise.
  2. Do not forward to anyone the messages containing false news of alarms or appeals for which disclosure is requested.
  3. Do not create, store and send advertising or promotional messages that are not related to the performance of work activities inside and outside the company domain
  4. Do not carry out massive communications through your email client, but only use the special instruments dedicated to email marketing (contact the IT function in case of need)
  5. Do not respond to messages apparently coming from senders considered “safe” (e.g. bank, mail, freight forwarders, etc.) and above all not to provide any personal data requested within these e-mails **or link to any links proposed in the message**.
* In all the situations described above, if there is any doubt about how to handle the message, remember to open neither the message nor any attachment, and contact the IT functions.
* It is necessary to securely archive emails messages that may engage the company with third parties or that have any legal value. Remember that it is possible to keep these messages on the email server, but this practice does not guarantee the characteristics of authenticity, integrity, reliability. In these situations it is advisable to contact the IT functions to assess the possible need for more suitable systems for secure storage, such as document management.

### Email - Absence management

On the basis of what was previously explained, it is specified that:

* 1. The content of incoming/outgoing email messages could be viewed by the Owner (through the appointed personnel), in the event of unforeseen and prolonged absence of the worker, if this were necessary for the continuity of the work activity.
  2. In the event of prolonged and expected absence, it would be good practice to activate the automatic answering service. The company has made available to each worker special functions (the so-called “out of office” or “off-site rule” alerts) through which the coordinates (phone or electronic) of a colleague can be sent automatically or an alternative structure to turn to. All users are therefore requested to use these services, thus preventing the possibility that their email Inbox should be consulted by other subjects.
  3. Alternatively and in all situations where it is necessary to guard the email Inbox for particular reasons of business operation, the user can identify a “trustee” who in his absence can check the emails and forward the necessary contents to who had urgency.
  4. In the event of failure to identify the trustee, the line manager is authorized to access the content of the messages or to have the automatic responder set up, through special personnel in charge. The user will be informed of the access to his email Inbox, at the first convenient opportunity.
  5. In the event that your mail has been consulted by a third party during your absence (as explained above), the access password must be changed by the user upon returning to the company.

# INTERNET POLICY

### Internet – General Rules

The systems connectivity to public networks is provided in order to best carry out their work activity.

Sporadic personal use is accepted only during non-working hours (e.g. during lunch breaks), within minimum time limits, comparable to other communication practices within the workplace, and in compliance with these guidelines, of all other company procedures and policies and the current legislation.

### Internet – Safe browsing rules

As required by the legislation on the protection of personal data, the company shall promote every appropriate organizational and technological measure, aimed at preventing the risk of improper use of company systems. Generally, preventing abuse shall be considered more important than identifying them, and therefore PREVENTIVE measures shall be preferred over the following REPRESSIVE actions.

Considering these principles, the company has adopted some organizational and technological security measures, and in particular:

1. Has identified the types of users to whom, for needs related to their profession, the use of email and/or Internet is granted.
2. Some computer devices have been installed for some time now, which reduce the risk of breaching your network from the outside
3. Has installed devices that limit and counteract any improper or dangerous uses of “browsing” on the Internet. In particular, dangerous sites are always blocked, with reference to black lists that are constantly updated and include categories such as pornography, pedophilia, violence, software piracy, copyright infringement, hacking and cracking, peer-to-peer, etc. Furthermore, during working hours, access to some categories of sites that are not relevant to the professional activity can be inhibited, and that can significantly influence the efficiency of the band (web mail, social networks, shopping, instant messaging).

The systems used guarantee a good level of protection of the corporate network with respect to illegal conduct; in any case, some basic rules are recalled:

1. It is forbidden to connect to sites such as WebChat, sites offering software protected by copyright and illegal activities in general.
2. It is forbidden to download and/or install independently on your own software station of any kind.
3. It is forbidden to browse the sites that may reveal the opinions of religious, trade union and health policies of the user since it is potentially suitable to reveal data of a sensitive nature.
4. Any form of registration is not allowed for sites whose contents are not related to work activities; participation, for non-professional reasons, in forums, chats or discussion groups is not allowed.
5. It is forbidden to carry out any kind of personal financial transaction, including remote banking, online purchases and the similar, except in the cases directly authorized by the Owner and in compliance with normal purchase procedures.

Users who use the company's Internet connectivity and browsing service are nevertheless informed of the fact that Fogliani has instruments, necessary for the security of IT systems, data and know-how, which record the addresses of the sites visited and the address of the workstation (IP) and therefore could be used to ascertain any conduct contrary to the policies for using the Internet and company instruments.

# VERIFICATIONS AND CHECKS

Fogliani and the other subsidiaries, as Owner of the data and IT tools used in the processing, reserves the right to carry out the checks it deems appropriate for the following purposes:

1. Protect the security of the corporate network and the integrity of IT instruments and data.
2. Avoid the commission of offences, implement preventive or defensive measures
3. Check the functionality of the system and IT instruments

Checking activities may also be carried out through specific technical or process audits, or by means of Vulnerability Assessment of the information system. For these checks the organization reserves the right to use external subjects.

It is specified, in any case, that the organization does not adopt “equipment for purposes of remote control of the workers' activity” (pursuant to Article 4, first paragraph, Law No 300/1970), including hardware equipment and software aimed at user control.

## Procedures for verification

In the event that a harmful event or a situation of danger to corporate security has not been blocked by the technical measures adopted, the company can adopt any measures that allow the verification of anomalous conduct.

Verifications will in any case respect the fundamental principles of relevance and not excess, and will normally be carried out in this way:

1. detection of the damaging event 🡪 anonymous verification on aggregate data 🡪 generalized notice (company or work groups)
2. repetition of the damaging event 🡪 verification on groups of stations/nominatives 🡪 warning/recall to the controlled group
3. repetition of the damaging event 🡪 individual verification 🡪 warning/recall nominative

The information registered or recordable automatically by the systems (Internet browsing log or email server log) can only be accessed by Fogliani's IT functions, formally authorized.

These appointees will carry out only the operations strictly necessary for the pursuit of the technical and safety purposes.

## Informative according to Article 13 of EU Regulation

Any personal data or belonging to particular categories, found on electronic instruments owned by the company, even if held or kept in violation of this regulation, will in any case be treated according to the confidentiality criteria provided by the law, solely for the purposes related to the control activity and/or any judicial protection of the company.

The software systems are configured in such way as to periodically and automatically cancel personal data relating to Internet access and online traffic, which conservation is not necessary.

Any prolongation of storage times is assessed as exceptional and shall take place only in relation to:

1. Specific technical or security requirements;
2. The indispensability of the data with respect to the exercise or defense of a right in Court;
3. The obligation to keep or deliver the data to comply with a specific request from the judicial authority or the Criminal Police.

## Penalties

Everyone will be held personally liable in the event of deliberate breach of the aforementioned rules, according to the applicable laws and contracts, including of a disciplinary nature.

Any penalties:

1. Verbal warning
2. Letter of recall inflicted in writing;
3. Fine;
4. Suspension from remuneration and service;
5. Disciplinary dismissal and with the other consequences of reasons and of the law;

Executive’s laws and/or collective negotiation are valid for executives, on the understanding that, for the most serious violations, the institution may proceed with the dismissal of the infringing executive.