INTERNATIONAL TELEMATIC UNIVERSITY UNINETTUNO

Guidelines for controls and security of company goods

(EU Regulation 2016/679)

UNINETTUNO
18/05/2018

TABLE OF CONTENTS

1 – LEGAL FRAMEWORK 2
Aims and area of application 2
Definitions 3

2 – INDENTIFYING WORK DEVICES 5
DEVICES USED BY THE EMPLOYEE 5
DEVICES FOR RECORDING ACCESSES AND ATTENDANCE 6

3 – MODES OF USE OF WORK DEVICES AND OF CONTROL ACTIVITIES FOR SECURITY AND COMPANY ASSETS PROTECTION NEEDS 7
Use of PC and of mobile devices 7
Use of application programs 8
Use of web browser and e-mail services 9
Use of distance teaching tools 11
Use of manual working devices 11

FOR APPROVAL 12

THE RECTOR 12

1 – LEGAL FRAMEWORK

AIMS AND AREA OF APPLICATION

THE INTERNATIONAL TELEMATIC UNIVERSITY (shortly UNINETTUNO), in its capacity of Controller of the treatment, has the legal obligation to implement appropriate technical and organizational measures to assure and be able to demonstrate, in case of need, that the treatment of personal data it performs is compliant with the principles and duties established by the EU Regulation 2016/679, concerning the protection of natural persons with regard to the processing of personal data as well as the free movement of these data.

Additionally, in its capacity of employer, it obliged to grant the respect of the dignity and freedom of its employees as provided for by art. 4 of the law n° 300/1970, as quoted below:

"*Art. 4. Audiovisual equipment.*

1. *Audiovisual equipment and other devices enabling the possibility of remote control of the employees' activities can be used exclusively for organizational and production needs, for work safety and protection of the company assets and can be installed further to a collective agreement entered by the Unitarian trade unions' representatives or by the company's trade unions' representatives. As an alternative, in the case of companies having production units based in various provinces of the same region or in more regions, the comparatively most representative trade unions' associations at national level can enter this agreement. Where there is no agreement, the equipment and devices mentioned in the first sentence, can be installed, further to an authorization of the local board of the Ispettorato nazionale del lavoro (National Work Inspectorate) or, as an alternative, in the case of companies with production units based within are of competence of more local boards, by the central office of the National Work Inspectorate. The provisions, as mentioned in the third sentence, have a definitive character.*
2. *The provision mentioned in paragraph 1 does not apply to the devices used by the employee to carry on his working tasks and to the devices used to register the accesses and attendance.*
3. *The information collected as per paragraph 1 and 2 are utilized with regard to employment relationship on condition that the employee is suitably informed about the modes of use of these devices and for performing the controls and in the respect of the provisions made by the Legislative Decree of the 30th June 2003, n° 196.*"

Consequently, by means of this document, UNINETTUNO sets itself the following objectives.

Primarily, that of identifying the devices utilized by the employee and the modes by which it performs the controls that aimed at protecting the company goods and information and grant their security.

Secondly, that of informing its employees and assistants.

Finally, that of documenting all these activities in order to assure and be able to demonstrate, if required, that the treatment in question are carried out in compliance with the above-mentioned Regulations and laws.

DEFINITIONS

As per paragraph 1 of art. 4 of the EU Regulation 2016\679, the following definitions are given:

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;
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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
restriction of processing	the marking of stored personal data with the aim of limiting their processing in the future;
profiling	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 analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;
pseudonymization	the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Filing system	any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
Controller	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
Processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
Recipient	a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients;
Consent of the data subject	any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
Personal data breach	breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
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;;
Representatives	the natural persons authorized to process personal data under the direct authority of the controller or of the processor;

2 – INDENTIFYING WORK DEVICES

DEVICES USED BY THE EMPLOYEE

As part of the performance of the working tasks by the employees and assistants of UNINETTUNO, even outside the company premises, the following devices are used:

a) The personal computers and relative peripheral devices available in UNINETTUNO's premises, regardless of the fact that they are connected to the company network;
b) The company network and all its hardware and software component allowing for communicating both within the local network and within geographical networks (Internet);
c) The physical and logical devices used to grant the protection of the network from unauthorized accesses and malfunctioning caused by computer viruses;
d) Physical and logical devises used to grant back services and restoration of the computer system and of its relative data;
e) Personal computers and other mobile devices (tablets, smartphones, etc.) entrusted to the employee by UNINETTUNO, including the relative set-up applications;
f) Basic operational programs and application programs needed for the production activity, both residing in the company servers and those made available by means of cloud computing services;
g) Company websites and relative information and intellectual contents;
h) chats, video-chats, audio and video-conferencing systems, forums set up in the e-learning platform and within the distance teaching activities, including the relative information and intellectual contents;
i) The individual e-mail account of the employee and the one that is shared with other employees, enabled in the company domain as well as the relative communication and message archiving service;
j) Individual authentication credentials to access the company network and/or application programs and/or cloud computing services;
k) Telephone switchboard and its individual devices and relative VOIP communication service;
l) Physical and logical archives with the documents included into them;
m) Furniture, furnishings and stationary.

Based on the duties and task entrusted to each employee the above-listed devices can by fully or partly required to carry on the working tasks.

Broadly speaking, during the working activity, it is admitted the use of working devices for personal purposes for a limited period of time, as long as this is actually possible and the functionality of the company devices and goods are not compromised, the rights of other subjects are not infringed and, in any case, this is not in contrast with contractual obligations towards the employer.

DEVICES FOR RECORDING ACCESSES AND ATTENDANCE

Devices to record attendance and in-bound and out-bound accesses of the employees that collect data through the manual use of a tool (magnetic badge) univocally assigned to each employee were installed in the company premises.

These devices are connected to the company network and transfer the collected data through an application software package (Speed attendance).

The program allows to process information in order to measure the duration of work performance in order to establish the exact quantification of the periodic remuneration as well as to correctly manage the working relationship in terms of the physical presence or absence of the employee in the workplace in compliance with the contractual rights and duties of both parties.

3 – MODES OF USE OF WORK DEVICES AND OF CONTROL ACTIVITIES FOR SECURITY AND COMPANY ASSETS PROTECTION NEEDS

USE OF PC AND OF MOBILE DEVICES

The PC entrusted to each employee in the fixed working station inside the company premises, as well as the mobile one, with all the mobile devices (tablets, smartphones, etc.) are the main tools to perform working tasks.

This is the reason why they must be used with the highest diligence and mainly for performing the working tasks.

It is admitted the use of PC or of a mobile device for personal purposes for a limited period of time, as long as this is actually possible and their functionalities are not compromised, the rights of other subjects are not infringed and, in any case, this is not in contrast with contractual obligations towards the employer.

It is possible that the devices are set up in such a way as not allow some functionalities, such as the connection to external peripherals or mass storage devices in order to avoid a possible conflict among apparatuses, the data mining or transmission of dangerous computer programs.

It is absolutely forbidden to alter, modify, disassemble, take away or damage, even involuntarily, the entrusted PC or mobile device. In case of breach, each employee may be called upon to account for his responsibilities also on a disciplinary level based on the seriousness of his behavior and of the effects caused to the company.

In case of breakdown or malfunctioning or of stealing of the mobile devices the employee must promptly notify his hierarchical head or the person in charge of the IT Area.

At the conclusion of the working performance or relationships, the employee is required to give back the mobile devices entrusted to him, also seeing to removing or eliminating all his confidential or personal information.

If he does not, the staff of the IT Area will immediately do so, soon after its redelivery.

USE OF APPLICATION PROGRAMS

The application programs as well as PC are the main working tools to carry on the working tasks.

This why they must be used with the highest diligence and in an exclusive manner or, according to the cases, mainly for carry on the working tasks.

It is admitted the use of the application programs for personal purposes within the limits of a mixed use and for a limited period of time, as long as its functionalities are not compromised, the rights of other subjects are not infringed and, in any case, this is not in contrast with contractual obligations towards the employer.

The access to the company network as well as the access to server-side application programs or made available through a cloud computing service must be always set up through an individual and univocal authentication procedures and always protected by a password. The password must not kept as confidential and must be regularly updated.

It is forbidden to access the system or application programs using the authentication credentials of another user, unless the sharing of the credentials is required by the specific configuration of the program or explicitly envisaged by the head of IT area.

Insofar as the password configuration criteria are decided by the company IT are, each employee will have to respect their previously communicated policies, whereas it will be his duty to learn and respect the above-mentioned criteria if they are decided and communicated by the producers or by external suppliers of application programs thanks to operational handbooks.

It is possible that the basic operational program or single application programs are configured in such a way as to enable certain functionalities, such as, by way of example: data download, programs setup, local copy, all this with the aim of avoiding any possible conflict among programs, the alteration of the system, data mining or transmission of dangerous computer programs.

It is absolutely forbidden to alter, modify or damage, even involuntarily, the computer programs used to perform the working tasks, the configuration decided by the system managers included. In case of breach, each employee may be called upon to account for his responsibilities also on a disciplinary level based on the seriousness of his behavior and of the effects caused to the company.

In case of breakdown or malfunctioning or of running of dangerous programs (viruses), the employee must promptly notify his hierarchical head or the person in charge of the IT Area.

At the conclusion of the working performance, if needed, the employee is required to log off from the application program.

USE OF WEB BROWSER AND E-MAIL SERVICES

The web browser programs and e-mail services make it possible, more than other working tools, for a double use.

From one side they are useful tools and, sometimes, necessary to perform the working task, from the other side they may be used for an almost concurrent personal use.

Consequently, it is necessary to give a detailed description of their use in a working environment.

The programs that allow for browsing geographical networks (Internet) can be used by the employee for personal purposes for a limited period of time, as long as this does not compromise the company information system and goods, the rights of other subjects are not infringed and, in any case, this is not in contrast with contractual obligations towards the employer.

Web browsing can expose the company information system and goods to the action of dangerous programs (viruses) or of other computer threats (intrusions and unlawful accesses) or it can allow the access to information contents, images, sounds and videos in breach of the law or of other parties' right.

Consequently, the use by the employee, both during the working task performance and during a temporary personal use, must always be made with caution, preferring the access of website well reputed in terms of reliability, security and respect of the law.

At present, the company information system is protected by antiviruses and firewall devices, set up by the IT are system managers that relatively prevent the action of dangerous programs or of other computer threats.

In addition, it is possible that the web browser programs and the anti-viruses and firewall devices are set up by the IT area system managers in such a way as to:

- Select websites considered more or less linked to the working tasks;
- Filter the browsing activity preventing the access to specific websites or the performance of some activities such as file downloading;
- Tracing, anonymously and for limited periods of time, the web traffic in order to detect the existence of a threat or of an action of dangerous programs.

This does not allow the employee to avoid the duty of adopting cautious behavior while browsing and to abstain from infringing the law or other parties' rights. In case of breach, each employee may be called upon to account for his responsibilities also on a disciplinary level based on the seriousness of his behavior and of the effects caused to the company.

The e-mail service represents the most delicate tool among those made available to the employee since, as the web browser programs, exposes the company information system and goods to the action of dangerous programs (viruses) or of other computer threats (intrusions or unlawful accesses) since, as well, allow for potentially more mixed use compared to others. Actually, an individual electronic mail account may be used also for personal correspondence purposes.

Within the company e-mail domain, it is possible to create individual or shared accounts.

Where the e-mail service is more largely used to perform the working tasks, shared e-mail accounts were set up and, therefore, they can be accessed by more people within the company with the main purpose of sharing the received messages and related annexes, in order to assure an efficient and continuous carrying on of the company activities their storing and further consultation, regardless of the availability of each individual employee.

In the case, instead, of assignment of an individual e-mail account linked to the company domain, the employee must adopt a caution behavior, based, as well, on the highest fairness and cooperation with UNINETTUNO in order to allow the performance of the working tasks.

Consequently, it is admitted the use of the employee's individual e-mail account, as long as this does not compromise the security of the company information system and goods, it does not infringe the rights of other parties and, in any case, this is not in contrast with contractual obligations towards the employer.

In the case in which the individual account is used during the teaching activities (diachronic distance tutoring), the use of this tool must always be based on the respect of the roles and dignity of the students.

During prolonged absence, it is envisaged the adoption of an automated answering system or the re-routing to another e-mail account of the company domain.

At the conclusion of the working relationships, the employee is required to remove or eliminate the personal e-mail messages and transmit to his hierarchical head or other person, specified by UNINETTUNO, those messages whose content is relevant for the continuation of the company activities.

To this end, the employee is invited by the Head of the Personnel Office to carry on these activities within 5 days. In case of breach of this duty of collaboration, the employee may be called upon to account for his responsibilities.

Past this deadline, his individual account is blocked by the system managers of the IT are and its contents is stored for 5 years without being consulted, unless necessary to protect a right in court or in a pre-litigation procedure.

The activity of the system managers of the e-mail account is recorded in specific log files in order to prove the compliance of the procedure.

In case they detect evidence of infringements of the duties related to the working relationship or a damage to the company goods, the system managers, further to written request of the employer, can consult the file log of the accesses to the accounts of individual and shared e-mail in order to identify any people responsible for these actions.

USE OF DISTANCE TEACHING TOOLS

The distance teaching activities implemented in the didactic cyberspace entail the use of specific tools for performing the synchronic distance tutoring tasks.

These tools are chats, video-chats, audio and videoconferencing systems, forums set up in the e-learning platform and in the distance teaching activities.

The use of these tools by the employee is allowed in at very limited extent, since they can interact, in real time, with a wide range of students and can interfere with the educational and training activities, besides being potentially detrimental for their dignity.

As a result, their use must always be based on the highest caution, on the respect of the roles and dignity of the students. In case of breach of these duties of collaboration and protection, the employee may be called upon to account for his responsibilities, also on a disciplinary level based on the seriousness of his behavior and of the effects caused to the company.

In addition, the use of these tools is subject to recording and archiving, also to allow their future use by students.

USE OF MANUAL WORKING DEVICES

The telephone set, stationary materials, furniture and furnishings of the workstation represent the traditional means to perform the working tasks.

It is admitted the use of these tools, in particular of the telephone set and of the stationary materials for personal purposes for a limited period of time and in a very limited amount, as long as this does not cause a significant economic damage to the employer and do not infringe the rights of other parties.

The employee must use the furniture, furnishings and cabinets used as a physical archive with the highest caution, protecting them from any damages or dangers. In case of breach of this duty of protection, the employee may be called upon to account for his responsibilities, also on a disciplinary level based on the seriousness of his behavior and of the effects caused to the company.

FOR APPROVAL

THE RECTOR

Document creation date: 18/05/2018

Document revision date: