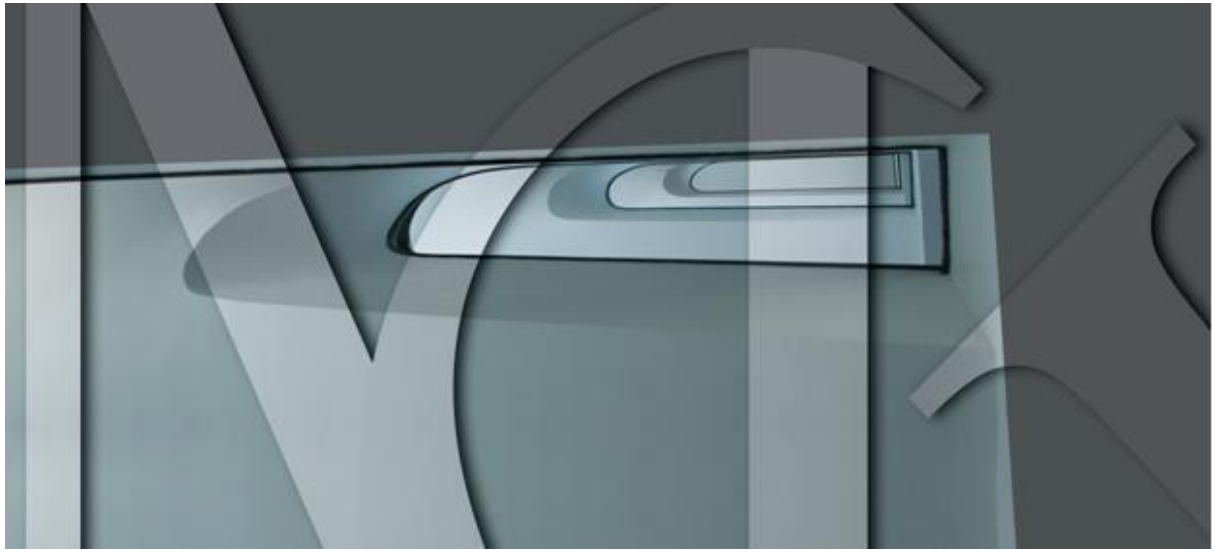
PRIVACY AND CORONAVIRUS:
Smart-Working
(focus: Associations - Foundations - Third Sector)

17 April 2020



Non-profit Associations - Foundations - Third Sector

Due to the COVID-19 emergency, in Italy many measures have been taken in the areas of labor law and social security law.

The new measures (only with some exception such as the social safety net regulation) did not pointed out a specific discipline relating to third sector's entities, regulating them jointly with private entities.

In Italy, both third sector's entities and private entities are considered as regular "employers" and, in such quality, must respect the Italian provisions governing the employment relationships and protecting the heath and safety of its employees.

The privacy law (GDPR – D.Lgs 196/2003) it is also applicable for the third sector entities and, in general for non-profit associations. Data subjects must be protected, regardless of the identity of the data controller. Due to COVID-19 Emergency, the Controllers must take all necessary measures to protect and ensure their personal data.

Smart-Working

Smart-Working is considered to be a new kind of work organization that enables a balance between an employer's production needs and the personal needs of individual workers.

The main characteristic of Smart-Working is to ensure ample flexibility in terms of working hours and place of work.

The aim of Smart-Working is in fact to empower workers by granting them greater organizational autonomy within a level of performance (generally) agreed upon with the employer.

Smart-Working therefore, differs from Teleworking which is not a flexible way of working, since it only provides a replacement of the workstation within the employer's premises with one that is at home.

The regulatory situation in Italy

The regulatory framework for Smart-Working has been defined by Law no. 81 dated 22 May 2017, which in a nutshell, provides that:

- Smart-Working is part of an employment relationship;
- In order to activate Smart-Working, a written agreement is required between the employer and the employee (wherein, moreover, the employer shall indicate some basic elements such as, for example, the duration of the agreement and the way its governing powers shall be exercised);
- Smart-Working shall be carried out within the maximum limits of time and duration indicated by law or collective bargaining and can be made without specific time constraints compatible with the work organization;
- Employers must guarantee workers the right to log off; and
- Employees who are Smart-Working shall be provided with a general and specific risk statement regarding the way the employment relationship is carried out.

The situation in Italy

The use of Smart-Working in the Italian market has been positively welcomed by larger companies/entities which have introduced this organizational method in order to increase welfare systems (more flexibility in some days) and reduce costs both for the employer (e.g. meal vouchers if paid when working on-site) and for the same worker (e.g. transport costs).

With the progression of the pandemic caused by Covid-19, the legislator identified the Smart-Working system as an emergency containment tool, allowing the worker to operate without entering into physical contact with colleagues.

Thus, the possibility to implement Smart-Working was introduced even without the prior signing of the individual agreement as well as by using a simplified procedure to send administrative communications.

The situation in Italy

Despite that Smart-Working is the system recommended by the legislator to deal with the Covid-19 emergency, given its extreme flexibility, in many cases, it is not considered to be the best and most reliable method of organization to ensure that employers' activities are carried out correctly (e.g. it would be better to apply Telework for workers who work from a fixed work station to be set up remotely by the employer).

In addition, following the Covid-19 emergency, many workers began operating without an agreement and without prior identification of specific work objectives. Therefore for employers who have not signed an individual agreement, it is opportune to prepare and send employees in Smart-Working, a brief indication of their main obligations, the rules of conduct to be followed and, if the case, the work to be executed and the timeframes to be observed in order to ensure that the work is carried out correctly.

Protection of the employee

Can employers control the activities of their employees in Smart-Working?

Art. 21 of Law 81/2017 provides that the agreement relating to Smart-Working regulates the powers exercised by the employer vis-à-vis the employee's work performance outside the employer's premises in accordance with Article 4 of the Law no. 300 dated 20 May 1970 (Workers' Statute).

The obligation to comply with art. 4 Workers' Statute outlined in Law 81/2017 provides that employees cannot be controlled from remote unless for (i) organizational and productive requirements, (ii) safety reasons and (iii) protection of the assets of the company/entity. In addition, in order for this control to be exercised, a trade union agreement or an administrative authorization must be signed in advance.

Protection of the employee

With reference to employees in Smart-Working, following the implementation of the Covid-19 containment provisions, the grounds for an employer to exercise control could be linked to organizational and productive requirements as well as to protect the assets of the employ/entity (e.g. customer data, financial data).

Therefore, under art. 4 Workers' Statute the employer that intends controlling its employees should sign a trade union agreement indicating the aforementioned reasons.

Furthermore, pursuant to this provision, the information collected could be used for all purposes relating to the employment relationship (including disciplinary ones) provided that employees are given the appropriate information regarding the tools used and the enforcement controls and in accordance with the privacy regulations.

Protection of the employee

Art. 4 Workers' Statute, under paragraph 2, however states that the trade union agreement (i.e. administrative authorization) is not required should the enforcement control be carried out on devices used by the employee to execute the work or on equipment recording logging and attendance, subject however to the informative note regarding the use of devices and enforcement controls.

This provision does not mean that the employer can implement indiscriminate remote control systems using the employer's devices allocated to the employee in Smart-Working, since in this case it needs to comply with the privacy provisions outlined in European (GDPR) and Italian legislation. In fact, while the use of digital technology, on the one hand allows restrictive measures imposed by the recent quarantine to be overcome, it shall be done with the necessary precautions and guarantees for the data of those concerned especially if implemented during an emergency situation such as the current one.

Protection of the employee

Any monitoring software shall be expressly indicated to the employee, and the employee shall receive adequate information from the employer regarding the software installed on the device. Data processing shall always be based on the core principles of the GDPR:

- Fairness: of course, the processing shall be carried out in accordance with the law and shall be lawful, both in terms of the legal basis and the modalities;
- Purpose and minimization: data processed shall be necessary for the purposes of the processing itself. Secondly, data that is not essential to control the employee shall not be processed.

Protection of the employee

In particular one should ask:

- Are the electronic devices provided to the employee essential to carry out the work?
- Is the software monitoring the activity essential to ensure the employee's best work performance?
- Has the functioning of the devices and monitoring systems been correctly indicated to the employee?

Less invasive measures should be favored, in order to balance work requirements with the interests of the employee (the Amazon scandal has become famous after it tried to introduce the famous 'electronic bracelets').

Protection of interested parties

Secondly, it is necessary to implement adequate measures to protect the personal data of customers/suppliers.

In fact, the personal data normally 'protected' within the company, both physically and virtually, are more easily accessible when 'agile work' is adopted.

The same, in fact, could be stolen, accidentally lost, be subject to abusive access or unwanted diffusion (imagine a company laptop being stolen or lost).

For the purposes of art. 32 of the GDPR, and therefore the adoption of **security measures**, the data controller shall implement the appropriate measures based on the type of data being processed.

Protection of interested parties

First of all, it is necessary to adequately **train** staff both in the use of devices (technological training) and on the rules governing the correct use when working outside the company.

Secondly, all the rules for data protection that should however be adopted in the work environment shall apply:

- Each device should have a password which shall expire on a periodical basis;
- Always install operating systems and security updates;
- Store personal data on a server or however protected by antivirus and firewalls;
- Do not save important documents on your desktop, but only on servers or secure locations;

Protection of interested parties

- The connection between the employee's device and the workplace (in most cases a VPN) should also be high-security and encrypted, so as to be immune to cyberattacks.
- It would also be opportune for the employee to sign a specific authorization for the processing of data in 'smart working' mode, in accordance with Articles 4, 29, 32 and 39 of the GDPR, which relate to specific instructions regarding the use of the device provided to the employee.
- If smart working measures have been implemented concurrently with the coronavirus emergency, each worker will need to be provided with unique credentials for remote access, and try to be provided with a stable and secure connection.

Provisions by the Garante (Italian Data Protection Authority)

- On 9 January 2020, the Garante sanctioned TIM following a complaint forwarded by trade unions. The subject of the complaint was the software through which the company monitored the activity of technicians 'on fields', considered to be detrimental to the privacy of the workers;
- Among the illegalities found by the Garante there is an irregularity in the information provided to employees, which failed to provide the exact period of data retention, as well as the illegitimacy of the retention period itself;
- In addition to the injunction order relating to the limitation of the processing carried out and the amendment of the informative note according to art. 13 of the Regulation, the Garante **fined TIM Euro 900.000** (in view of the seriousness of the violations) by publishing the provision on the Garante's website.

Provisions by the Garante (Italian Data Protection Authority)

- On 23 January 2020, the Garante sanctioned the Azienda Ospedaliero Universitaria Integrata of Verona, despite the latter having notified breach of personal data it controlled as per art. 33 of the GDPR;
- It has been established, in fact, that some of the Company's employees, using a workstation left unattended by a doctor, had accessed their colleagues' medical records in a complete illegitimate way;
- The investigations carried out by the Garante showed that the technical and organizational measures taken by the hospital had not proved suitable to ensure adequate protection of the patients' personal data and to protect them from unauthorized processing, thus leading to illicit data processing;
- For these reasons, the Company **was fined Euro 30.000**, as it should have monitored the data it controlled in a more responsible way.

Practical recommendations

In light of the brief indications provided in the previous slides, employers who have been forced to urgently implement a Smart-Working regime as a result of the Covid-19 outbreak are advised as follows:

1. If a Smart-Working Agreement has not been signed pursuant to Law 81/2017, send employees in agile working regime a **brief description of the main rights and obligations of employees in Smart-Working** as well as the activities to be carried out;
2. prepare and send employees **an informative note on the use of the IT devices** allocated to carry out their work, indicating any enforcement controls carried out by the same devices;
3. prepare and send employees **a document to obtain their authorization for the processing of personal data collected during the agile working period**, as well as an informative note relating to the processing of data.

The above documents shall be sent through a traceable system (e.g. email) and must be signed by employees.

OUR TEAM IS AVAILABLE FOR ANY ADVICE AND CLARIFICATION

FILIPPO MONTANARI
Associate
Verona
Tel. +39.045.8010911
f.montanari@macchi-gangemi.com

GIULIA VERGA
Partner
Verona
Tel. +39.045.8010911
g.verga@macchi-gangemi.com

ENRICO STORARI
Partner
Verona
Tel. +39.045.8010911
e.storari@macchi-gangemi.com

MARCO LANZANI
Partner
Milan
Tel. +39.02.763281
m.lanzani@macchi-gangemi.com

ELISA NOTO
Partner
Rome
Tel. +39.06.362141
e.noto@macchi-gangemi.com

FILIPPO BODO
Associate
Milan
Tel. +39.02.763281
f.bodo@macchi-gangemi.com

OUR OFFICES

00197 **ROME**
Via G. Cuboni, 12
Tel +39.06.362141
Fax +39.06.3222159
roma@macchi-gangemi.com

20122 **MILAN**
Via G. Serbelloni, 4
Tel +39.02.763281
Fax +39.02.76001618
milano@macchi-gangemi.com

37121 **VERONA**
Via G. Garibaldi, 17
Tel +39.045.8010911
Fax +39.045.8036516
verona@macchi-gangemi.com

75008 **PARIS**
38, Avenue Hoche
Tel +33 (0) 1.53757900
Fax +33 (0) 1.5375001
paris@macchi-gangemi.com

SW1Y4JS **LONDON**
33, St. James's Square
Tel + 44 (0) 20 3709 6000
Fax + 44 (0) 20 3709 6014
london@macchi-gangemi.com