Gatti Pavesi Bianchi

Data Protection and Cybersecurity

DATA PROTECTION RULES DO NOT PREVENT MEASURES TAKEN TO FIGHT COVID-19

On 11 March 2020, the Italian Government, in light of the further and exceptional worsening of the epidemic COVID-19, recommended employers to take proper anti-contagion measures (Prime Ministerial Decree dated 11 March 2020 art. 1 n. 7 lett. d); which reads: "*with regard to industrial and professional activities, it is recommended the adoption of anti-contagion safety protocols and, in cases when this is not possible, the respect of one-meter distance between people as main safety measure, along with the adoption of individual protection tools*".

On 14 March 2020, the Government and the main stakeholders (companies representatives and labor unions) issued a further protocol stating measures to oppose and contain the spread of Covid-19 virus in workplaces (hereinafter referred to as the "Protocol") includes a list of obligations and recommendations regarding the processing of employees' personal data, resulting from the adoption of such safeguards. Among these, specific attention has been devoted to the possibility of locating the devices for real-time detection of the body temperature of employees and visitors who access the company.

The measures suitable for ensuring safety on the workplace can be summarized as follows.

Information duties

To be implemented by means of posting warnings on company premises to inform visitors and employees about:

(i) obligation to stay at home in case of temperature (over 37.5) or other flu symptoms and obligation to notify the symptoms to their doctor;

(ii) ban on entering and remaining within the company premises if there are dangerous conditions after the entry (including contacts with people who have been tested positive in the last 14 days) and to disclose this situation immediately;

(iii) obligation to respect safety measures (in particular distances and hygiene);

(iv) obligation to notify immediately to the employer the outbreak of flu symptoms of any kind during working hours.

Prevention measures (measurement of temperature by Termoscan)

In order to regulate the entry of employees and visitors within the company premises, the employers may:

(i) measure employees' body temperature and forbid access to those who have a higher value than 37.5, even without the intervention of national health service or civil protection personnel, as initially indicated by the *Garante* in its recommendations dated March 2 (when the emergency was not so dramatic);

(ii) order temporary isolation of the employees and provide the same with a mask (employees in this condition must not go to the emergency department or to the infirmary, but must contact the doctor and follow his instructions);

(iii) inform the staff and those who intend to enter the company premises that the access is forbidden for the subjects who, in the last 14 days, have had contacts with people who have been tested positive for COVID-19 or as well come from areas at risk according to WHO indications.

With specific reference to body temperature measurement, these guidelines should be followed:

- employers may detect the temperature **but not record data**; it is possible to identify the employee and record the temperature measurement only to document the reasons that prevented his/her access to the company premises;
- employers **should inform, also orally, the employee indicating that among the purposes of processing there is the prevention of COVID-19 infection and that the data retention period is related to the state of emergency**;
- employers **should adopt specific security measures, appointing internal processors in charge of the processing and provide the latter with specific instructions**;
- **implement suitable measures to protect the employee's privacy and dignity during his/her temporary isolation.**

Our practical tips:

(i) Place information signs regarding safety procedures in the areas immediately in front of the Termoscan and in other places such as cafeterias, operating areas and toilet rooms.

(ii) Prepare specific notices, which have to be concise but complete, and indicate the essential elements identified above.

(iii) Within industrial units with a significant number of employees, make available the notices in paper and, when possible, deliver them to the data subjects.

(iv) Prepare specific instructions for the employees who will be in charge of the processing of sensitive data collected through Termoscan.

(v) Verify that data protection security measures are properly implemented and adequate to avoid data leaks.

(vi) Whether the employer chooses to request a self-declaration from the employee related to potential risk exposure (e.g. contacts with subjects resulted positive to COVID-19 or origin from areas at risk according to WHO indications) this will be considered as processing of personal data and therefore, must be preceded by prior information - also orally - and must be accompanied by the adoption of specific security measures (including the appointment of duly trained subjects in charge of the processing).

Cybersecurity: smart working and protection of personal and non-personal data

With reference to smart working methods, which are strongly recommended by the Prime Ministerial Decree and which have already been adopted by many Italian companies, it is necessary that they are as much as possible built with the aim to protect company data, whether personal or non-personal.

Remote access to the corporate network, if not adequately protected, arises two criticalities: risks of suffering data breaches, and risk of disclosure of secret Know How.

Our practical tips:

1. Protection of devices that allow connection to the corporate network: we remind you that devices that remotely connect to corporate network are commonly known as “endpoints”, and must meet certain requirements

(i) Strong-password: the use of complex passwords, consisting of numbers, upper and lower case letters, special characters, etc. is strongly recommended.

(ii) Encryption of data saved on the device: to protect the data contained in the PC hard disk it is important to encrypt the hard disk. In this way, in the event of theft / loss of the PC, the data would not be accessible to some attacker.

(iii) Update of the operating system, antivirus, and antispam: the operating and protection software must be constantly updated in order to guarantee the best possible protection of the device against any malware or viruses.

2. Protection of access to the corporate network:

(i) Virtual Private Nework (VPN): VPN is a connection technology that allows endpoints to connect securely - typically VPNs use encrypted connections - to the company's local network using the public Internet. Through the VPN, endpoints access all shared resources as if they were physically connected to the corporate network.

(ii) Strong-Authentication: it is a protection system that makes hackers' remote access to the corporate network more complicated. In fact, to log in, not only the password is sufficient but also another code or digital certificate or biometric fingerprint.

(iii) Identity and access management: access to shared resources cannot be complete must be guaranteed mainly on the basis of:

- the role: it is possible to identify and separate the tasks of employees and collaborators in order to guarantee access based on their role (for example, accounting will not have access to human resources documents and viceversa).

- the attributes: accesses can be guaranteed through other customized attributes, for example the access time or to the location where files are saved.

TEAM

Massimiliano Patrini
Massimiliano.patrini@gpblex.it

We provide assistance to the Firm's clients by highlighting the value of their intangible assets, in the various sectors of Industry and Services (fashion, luxury, advertising, e-commerce, banking and finance, mechanical, chemical and pharmaceutical), ensuring comprehensive advice in each area whether it is domestic or international, in the processes of technology transfer, acquisition and merger of companies, negotiation of license agreements and sale of industrial property rights. Having acquired vast experience in judicial matters, has allowed us to support, defend and represent our clients in any litigation relating to trademarks, design, trade secrets, unfair competition and copyright.

Addressing issues related to data protection, enhancement and management of personal and non-personal data, and the new sector of technology law.

Milan
Piazza Borromeo, 8
20123 Milano (MI)
Tel. +39 02 8597 51
Fax +39 02 8094 47
studio@gpblex.it

Rome
Piazza dei Caprettari, 70
00186 Roma (RM)
Tel. +39 06 6813 4961
Fax +39 06 6813 4701
studioroma@gpblex.it