Nctm

Client Alert | Corporate & Commercial

Italy

COVID-19: issues of concern to businesses in the field of personal data protection*

March 2020

***IMPORTANT NOTE**: this *memorandum* is updated as of 31 March 2020 at 1 pm. Since the state of emergency and the related regulatory framework are constantly evolving every day, the contents of this *memorandum* may be subject to continuous changes.

1. Foreword and reference framework

Following the increase in cases of Coronavirus COVID-19 infection in various areas of the world in addition to Italy, the Italian Government decided to adopt extraordinary and urgent measures to counter the spread of the virus and to strengthen the national health system, starting with the state of emergency declaration made by the Council of Ministers on 31 January 2020.

For further information on the measures adopted by the Italian Government and for any further updates, please consult the relevant institutional websites of the Italian Government and of the Ministry of Health, the web pages set up by the individual Regions as well as the updates for businesses and explanatory notes provided by Confindustria, including those provided by Assolombarda. See also the information page prepared and updated by the Italian Data Protection Authority.

2. Issues of concern to businesses in the field of personal data protection

The protection of personal data is of central importance in the context of the measures to combat the spread of COVID-19.

Several of the possible measures to prevent infection that have been considered in the last few weeks (e.g. the provision of questionnaires to ascertain the state of health of workers, the release of self-declarations, the detection of body temperature upon accessing company premises, the adoption of digital contact tracing measures, in respect of which the Government and the Data Protection Authority are currently cooperating) indeed involve the processing of personal data of citizens, and particularly workers, including health data.

Nctm Studio Legale
Via Agnello 12
20121 Milano

T +39 02 72551.1
F +39 02 72551.501
C.F e P.IVA: IT 12988470154

As is known, the legislation on personal data protection, besides requiring compliance with the general principles set out in Article 5 of Regulation (EU) 2016/679, known as the "GDPR" (and, particularly, with regard to the processing at issue, with the principle of proportionality and data minimisation) and with general information and data governance requirements, makes the lawfulness of processing conditional upon the existence of one or more of the conditions under, respectively, Article 6 of the GDPR, as to "common personal data", and Article 9 of the GDPR, as to special categories of personal data (to be interpreted in the light of the requirements set out by the Authority by means of general authorisations, as amended following the entry into force of the GDPR and the amendments to Legislative Decree No. 196/2003 introduced by Legislative Decree No. 101/2018).

On the one hand, the processing of "common personal data" (such as, for example, the data coming from the collection and subsequent processing of information about the worker or visitor movements or contacts with people from the infected areas, etc.) can well be justified by the employers' legitimate interest in protecting their personnel from possible risk factors.

The processing by employers of health data should be based on the condition set out in Article 9(b) of the GDPR, which allows the processing of health data when it is "*necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, insofar as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject*".

However, the processing of health data in the performance of obligations regarding health and safety at work can - in principle - only be carried out as part of the performance of health surveillance activities, which the Safety Consolidation Act entrusts exclusively to the competent doctor. Any collection of health data shall therefore be conditional on the carrying out of a new risk assessment by the employer and the updating, as a result of such assessment, of the company's health protocol. Accordingly, only the competent doctor should be allowed to carry out the processing, either alone or - if necessary - through his or her own expressly authorised assistants.

Nevertheless, in consideration of the current emergency, the above regulatory framework has - for the time being - been superseded by the provisions contained in the "*Shared Protocol for the regulation of measures to combat and contain the spread of the COVID-19 virus in the workplace*" ("**Protocol**"), entered into, pursuant to Article 1, paragraph 1, No. 9 of the Decree of the President of the Council of Ministers of 11 March 2020, by the main employers' associations and unions. Although such document does not have the force of law but contains the main recommendations shared by the parties aimed at containing the COVID-19, it is unlikely that the activities allowed thereunder may be challenged at a later date by the businesses that have implemented the same, as it was substantially endorsed by the Government and, among others, by the Data Protection Authority.

That being said, the Protocol allows businesses to carry out the following activities and, therefore, the related processing operations involving personal data (including health data):

a) measurement of body temperature before accessing company premises (if higher than 37.5°, access is not allowed), with the legal grounds for that being identified in the obligation to implement the security protocols against the spread of COVID-19 pursuant to Article 1, No. 7, d) of the Decree of the President of the Council of Ministers of 11 March 2020 and the end of the state of emergency being referred to as the conservation period. Temperature data should not, as a rule, be recorded, but it is permitted to identify the person and record such data if the temperature exceeds the threshold set out in order to document the reasons for preventing access to the company's premises. In any case, the relevant information must be provided to the person concerned. The relevant data shall not be disclosed or communicated to third parties, unless expressly provided for by law (for example, if so requested by the health authority for the reconstruction of the chain of close contacts of any person tested positive for COVID-19);

b) request for a statement whereby one confirms that he/she is not coming from at-risk areas and that in the last 14 days has not been in contact with individuals tested positive for COVID-19. Such processing is likewise based on the obligation to implement the security protocols against the spread of COVID-19 pursuant to Article 1, No. 7, d) of the Decree of the President of the Council of Ministers of 11 March 2020. It is also clarified that only the data that is necessary, adequate and relevant for the purpose of preventing the spread of the virus shall be collected and processed (for example, if information is requested on contacts with people tested positive for the virus, it is necessary to refrain from requesting additional information regarding the person tested positive);

c) request for a self-declaration by a person who has developed COVID-19 symptoms while at the company premises by reporting to the personnel department. Following such reporting, the person must be temporarily isolated and the company must notify the competent authority thereof, cooperating with the latter to identify any person who may have had “close contact” with the isolated person. For the duration of the investigation period, the company may ask possible close contacts to leave the premises, as a precautionary measure.

It should be noted that the above provisions are supposed to apply to external visitors too.

Following the adoption of the Protocol, Confindustria prepared an explanatory note aimed at assisting companies with the application of the same in such context, further indications are specified regarding the role of the competent doctor, who is *inter alia* required to notify the employer of any situations of particular “fragility” and current or past underlying pathologies of employees and, accordingly, the employer shall procure their protection in accordance with privacy requirements.

Finally, for the sake of completeness, it is also worth mentioning the "*Statement on the processing of personal data in the context of the COVID-19 outbreak*", adopted by the European Data Protection Board ("**EDPB**") on 19 March 2020.

First, the EDPB confirms the principle that data protection rules do not hinder the measures taken in the fight against the coronavirus pandemic. Nevertheless, data controllers and processors must ensure the protection of the personal data of the data subjects, the general principles of law must in any event be respected and, finally, any measure taken in such context must not be irreversible. In other terms, emergency may legitimise restrictions of freedoms provided that such restrictions are proportionate and limited to the emergency period.

That being said, concerning data processing in the employment context, the EDPB confirms that the employer may process specific health information concerning employees and visitors, in the Covid-19 context, only to the extent allowed by national law.

Concerning, in general, the processing of location data, compliance is required with the provisions of Directive 2002/58/EC (known as the "**e-Privacy Directive**"), which in principle allows the use of location data the operator when made anonymous or with the consent of individuals. However, Article 15 of said Directive enables Member States to introduce legislative measures to safeguard public security insofar as they are necessary, appropriate and proportionate measures within a democratic society.

More specifically, the Authority seems to allow the use by Member State governments of mobile location data as a possible way to monitor, contain or mitigate the spread of COVID-19, which may imply, for instance, the possibility to geolocate individuals or to send public health messages to individuals in a specific area. Nevertheless, public authorities should first try to process location data in an anonymous way, processing data aggregated in a way that individuals cannot be re-identified. When data anonymisation measures are not adopted, the Member State concerned will be required to put in place adequate safeguards such as providing individuals of electronic communication services the right to a judicial remedy. In any event, the Member State should always prefer the least intrusive solutions that are sufficient for prevention purposes.

*** *** ***

This article is for information purposes only and is not, and cannot be intended as, a professional opinion on the topics dealt with.

For further information please contact your counsel or send an email to the following address: corporate.commercial@nctm.it or to the following lawyers: Paolo Gallarati or Francesca Bonino.

The following associates contributed to the drafting of this memorandum: Virginia Paparozzi, Giulio Uras and Lucrezia Lorenzini.