COVID-19 AND DATA PROTECTION

SOME CONSIDERATIONS FOR PRIVACY IN THE COVID-19 CONTEXT

The General Data Protection Regulation (GDPR), which is applicable since 25 May 2018, governs the processing of personal data throughout the European Union (EU). GDPR aims at ensuring a consistent and high level of data protection within the EU without jeopardising the free flow of data within the EU.

The GDPR has replaced Directive 95/46/EC of 24 October 1995 in force since 1995, and it superseded national data protection laws, including Law 67/98, of 26 October 1998. Along with the GDPR, Law 58/2018, of 8 August 2019, which implements some local specifics, is also in force in Portugal (GDPR Local Law).

Public and private entities are taking exceptional measures to prevent and mitigate COVID-19 across the EU, including in Portugal, where it was decreed a situation of state of emergency on 19 March 2020 and extended, at least, until 2 May 2020.

In this context, the Portuguese Data Protection Authority (DPA) has issued four papers:

(a) Resolution number 2020/170 of 16 March 2020, whereby all formal regulatory actions in connection with outstanding information request backlogs are suspended; and

(b) Three guidelines:

(i) Guidelines of 2 April 2020 on the use of video surveillance systems and alarms in the COVID-19 context, where the DPA stresses that private security companies are prohibited from carrying out activities falling into the scope of the exclusive powers of judicial or police authorities, including border control and the prevention and repression of crimes in public places;

(ii) Guidelines of 9 April 2020 on the use of distance learning technologies considering that Portuguese students are taking e-learning classes from their homes; and

(iii) Guidelines of 17 April 2020 on remote control means of employees under a distance work regime issued in response to several questions on the use of software for control of employees' performance in teleworking, and the imposition on employees of a permanent connection to the video camera. The DPA clarifies that the use of such software tools is disproportionate and infringes data protection principles, and that labour rules prohibiting distance control means of employees' activity remain applicable.

Apart from these four initiatives, no additional information is available in connection with data protection and COVID-19. Inversely, other EU data supervisory authorities, for instance, in the UK and Germany, have

disclosed a set of materials and FAQs at their websites to respond to data protection questions arising from the current situation.

The current situation may involve the processing of different types of personal data, including special categories of personal data, such as health data, namely within an employment context. In a COVID-19 scenario (not only at the current stage of spreading, but also at subsequent stagnation and mitigation stages), the processing of personal data may be necessary for compliance with employers' statutory obligations, e.g. obligations relating to health and safety at the workplace, or to the public interest, e.g. the control of diseases and other threats to health.

Bearing in mind that several questions may arise within an employment context (but not limited to), we have prepared a list of FAQs to help organizations to be able to respond to such new challenges.

1. May employers collect personal data of employees to prevent the spreading of the COVID-19 virus at the workplace? In affirmative case, what personal data is the employer allowed to process in this context?

Yes, employers may collect personal data of employees in order to prevent the spreading of the virus at the workplace to the extent that it is required to fulfil employers' statutory duties (e.g. duty of care) and to organise the work in line with the Portuguese legislation, namely Portuguese labour rules.

The criteria should be whether the processing is necessary for a given purpose (e.g. processing that is necessary for the protection of the health of employees and for compliance with statutory reporting obligations), and the implementation of the GDPR's principle of data minimization.

In principle, the collection of the following data will not raise major issues: name, current contact information, contacts with other persons within the organization, previous or intended stay in a high risk area, previous contacts with allegedly infected persons or whether a person is symptom-free.

Inversely, health data, which is considered a special category of data, is subject to restrictions and that require an adequate interrelation between the GDPR, the GDPR Local Law and the Portuguese labour rules, as detailed below.

2. In these circumstances, what requirements must employers comply when they carry out processing of employees' personal data?

Employers may collect and process personal data of employees, including health information, to determine whether (i) they are infected or have been in contact with an infected person, or (ii) they were in a high-risk area during the relevant period.

Employers should inform employees about COVID-19 cases and take protective measures, but they must not disclose more information than it is required.

Employers must keep employees informed about cases in their organisation, but they must not name individuals. The disclosure of personal data of infected persons (confirmed and suspected) to inform colleagues or externals is only lawful on condition that it is strictly necessary under exceptional circumstances to know the identity of that person, in order to mitigate the spread of the COVID-19 and allow employees to take relevant safeguards. In these very exceptional cases (where it is necessary to reveal the name of the employees who contracted the virus, e.g. in a preventive context), the concerned employees shall be informed in advance and their dignity and integrity shall be protected.

3. What is the relevant lawful basis for such data processing by employers?

As regards employees, the relevant lawful basis is the GDPR's legitimate interests (Article 6/1(f) GDPR).

Where health data is processed, the relevant legal basis should be the GDPR's employment and social protection legal basis, i.e., processing that is necessary for the purpose of carrying out the obligations and exercising specific rights of the employer or of the employees in the field of employment and social security and social protection law (Article 9/2(b) GDPR).

As regards local law, namely the labour law and the GDPR Local Law, we should stress the following rules:

(a) Article 28/1 of the GDPR Local Law states that the employer may process employees' personal data for the purposes and within the limits set out in the Portuguese Labour Code;

(b) Article 17/1 (b) of the Portuguese Labour Code states that the employer may not ask for the employee to disclose health data, save as when exceptional circumstances related to the professional activity may justify such disclosure and relevant grounds are provided in writing by the employer. Health data are provided to a medical doctor, who may only inform the employer on whether the employee is or not able to performance their job functions; and

(c) Article 29/2 of the GDPR Local Law states that special categories of data, namely health data, may be processed for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health, and that suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy, must be adopted.

This means that the employer's legitimate interests' legal basis and, for health data, the employment and social protection legal basis, result from the general duty of care of the employer toward their employees. Health date must be processed by the employer, through a medical doctor subject to professional secrecy, which means that health data may not, in principle, be disclosed to other employees, unless in exceptional circumstances and insofar it reveals necessary to avoid the spreading of the COVID-19 at the workplace.

Under the duty of care, the employer must ensure the protection of the health of all employees. This also includes carrying out an appropriate response to the dissemination of the COVID-19, for prevention and traceability purposes (i.e., subsequent prevention toward contact persons).

It should be also noted that the GDPR includes derogations to the prohibition of processing of certain special categories of personal data, such as health data, where it is necessary for reasons of substantial

public interest in the public health area (Article 9/2(i) GDPR), on the basis of EU or local law, or where there is the need to protect the vital interests of the individuals (Article 9/2(c) GDPR). As recital 46 GDPR states some types of processing may serve both important grounds of public interest and the vital interests of the individuals as for instance when data processing is necessary for monitoring epidemics and their spread.

In turn, employees' consent cannot be considered as a lawful basis, as, in an employment relationship, there is a clear imbalance between employees (data subjects) and the employer (controller). It is unlikely that employees' consent is freely given in the context of an employment relationship.

4. May employers process personal data of workplace visitors for COVID-19 related purposes?

Yes, employers may process personal data of workplace visitors for COVID-19 related purposes to determine whether (i) they are infected or have been in contact with an infected person, or (ii) they were in a high-risk area during the relevant period, and to the extent that the measures to be adopted are proportionate.

As regards visitors, measures against third parties that require the processing of health data can be justified based on the GDPR's lawful basis regarding processing that is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health (Article 9/2(i) GDPR).

The consent of visitors (data subjects) can only be considered as a lawful basis for COVID-19 measures if they comply with all consent requirements, including if visitors are informed about the data processing and can provide consent about the measures voluntarily. This means that visitors should be aware at least of the identity of the data controller (the organization) and the purposes of the processing for which the personal data are intended in the context of COVID-19.

5. Are private mobile phone numbers and email addresses of employees allowed to be collected?

During the pandemic, employees may work from home more frequently than usual and they can use their own device or communications equipment. The collection of private mobile phone numbers and email addresses of employees may be necessary and hence lawful if they are to be used to ensure their "ongoing availability" during the current COVID-19 crisis, namely if employees are working through a distance work regime.

It may be also necessary if, for instance, an overload of the organization's IT infrastructure makes it necessary to communicate within the employer and/or other employees. In this case, care must be taken to ensure that no sensitive data is disclosed by means of "unsafe" communication means, namely email services, where there is a risk of unauthorized access to data by third parties.

Employers and employees need to consider the same kinds of security measures for homeworking that they use in normal circumstances, for instance, hardware and software encryption, a two/three-level password authentication system, keeping access log files. The data may only be used for the intended purpose and must be deleted immediately after the processing purpose has ceased to apply.

6. May employers use technological solutions for remote control of their employees' performance through a distance work regime? May videoconference calls between employees or between the employer and employees be recorded?

According to recent guidelines issued by the DPA, the general rule prohibiting the use of means of remote surveillance to monitor employees' performance is fully applicable in a distance work context. The same conclusion would always be reached by applying the principles of proportionality and minimization of personal data, since the use of such means implies an unnecessary and excessive restriction of employees' private life.

For this reason, technological solutions for remote control of the employee's performance are not allowed. Examples of this are software that, in addition to tracking working time and inactivity, records the Internet pages visited, the location of the terminal in real time, the uses of peripheral devices (mousse and keyboards), capture images of the working environment, observe and record when the access to an application is initiated, control the document in which the employee is working and record the respective time spent on each task (e.g., TimeDoctor, Hubstaff, Timing, Manic Time, TimeCamp, Toggl, Harvest). This type of tools manifestly collects excessive personal data from employees, promoting the work control at a higher level than that which can legitimately be carried out at the employer's premises. The fact that the work is being carried out from home does not justify a further restriction towards employees. To that extent, the collection and subsequent processing of such data violates the principle of minimisation of personal data.

Similarly, it is not allowed to require the employee to keep the video camera on a permanent basis, nor, it is, in principle, allowed to record videoconferences between the employer and employees.

Despite the prohibition of the use of such tools, the employer keeps the power to control the activity of the employee, which it may do, namely, by setting objectives, creating reporting obligations as often as it deems necessary, scheduling meetings by videoconference.

7. May employees' files be processed in an employee's home office (e.g. in the home office of the Human Resources staff)?

The processing of employees' files in an employee's home office can only take place in exceptional circumstances if it is strictly necessary and to the extent that technical and organizational measures are taken to protect personal data, including, for instance, hardware and software encryption, a two/three-level password authentication system, keeping access log files, not printing in the home office.

If you need any further clarifications or assistance in any questions on data protection matters, please do not hesitate to contact us.

Macedo Vitorino e Associados

www.macedovitorino.com