Personal Data Processing in the context of Covid-19

March 31
2020

KARATZAS
& PARTNERS

Personal Data Processing in the context of Covid-19

I. General Remarks

In the midst of the COVID-19 coronavirus pandemic and in an effort to mitigate its effects and delay its spread, governments, as well as public, private, and voluntary organizations are already adopting measures that involve the processing of personal data (such as name, address, workplace, travel details) of individuals, including also 'sensitive' personal data (such as data relating to health).
To this end, both the Hellenic Data Protection Authority (HDPA), and the European Data Protection Board (EDPB) issued guidelines concerning personal data processing in relation to measures taken by private entities and public authorities in order to address the COVID-19 crisis.

First, the HDPA clarified that details concerning the state of health of a natural person (his/her state as bearing the coronavirus, his/her staying at home due to the virus, the identification of the disease's symptoms, etc.) are considered sensitive data, i.e. specific category personal data subject to a stricter protection regime, as opposed to travel information that are not considered sensitive, but may, under certain conditions, constitute mere personal data. The HDPA also added that the oral information regarding the infection of an individual by coronavirus or that his/her body temperature has been measured above normal constitute personal data, but the relevant legislation (the General Data Protection Regulation ('GDPR') and Greek law 4624/2019) does not apply if the above information has not been subjected to a filing system or automated processing. In particular the HDPA underlines that *"protection of personal data is not an absolute right but must be evaluated in relation to its function within the society and weighed in relation to other fundamental rights and in accordance with the proportionality principle."*

II. Principles relating to processing of personal data

The data protection rules do not prevent private entities and public authorities from the adoption of measures to fight the coronavirus pandemic, provided that the data processing is **lawful** and the data processing principles, as set out in Article 5 and 6 of the GDPR, such as **data minimization, transparency, data security, and data retention** are upheld.

A. Lawfulness

Processing of personal data by both corporations and public authorities shall be lawful only if and to the extent that at least one of the legal bases under art. 6 and 9 GDPR apply.

○ Public Authorities

The public authorities constitute data controllers who process sensitive or mere personal data as part of the necessary measures taken for the purpose of avoiding the risk of the occurrence or spread of the coronavirus and the ultimate protection of public health.

In such cases, the appropriate legal basis for the processing of simple personal data are the ones provided for under art. 6 par. 1c' (compliance with a legal obligation), d' (protecting the vital interests of the data subject or of another natural person), e' (processing is necessary for the performance of a task carried out in the public interest or in the exercise of public power).

Likewise, with respect to the processing of sensitive data, the applicable legal bases are the ones detailed under art. 9 par. 2b' (carrying out obligations and exercising specific rights in the field of employment, social security and social protection law), e' (processing relates to personal data which are manifestly made public by the data subject), h' (processing for the purposes of preventive or occupational medicine, for the assessment of the working capacity, medical diagnosis, the provision of health or social care or treatment etc.) and g' (processing public interest purposes in the field of public health). Recital 52 of the GDPR explicitly makes reference to the prevention or control of communicable diseases as a specific example for the processing of special categories of data in the public interest.

- **Private Entities**

In the employment context, law 3850/2010 and other provisions in force establish employers' responsibility, on the one hand, to ensure health and safety of their employees by undertaking preventive measures for guaranteeing a safe and healthy working environment, while employees, on the other hand, are also required to apply health and safety rules including to report immediately any incident that may pose a direct and serious threat to the health and safety.

In light of this, employers may **lawfully** process personal data under the appropriate legal basis of art. 6 GDPR. In particular, employers may proceed to such action, in case processing is necessary for them to comply with their foregoing obligations (art. 6 par. 1c') or in order to protect the vital interests of their personnel (art. 6 par. 1d'), or processing is necessary for the performance of a task carried out in the public interest (art. 6 par. 1e'). In this regard, the monitoring of epidemics is a type of processing, which may serve important grounds of the vital interests of the data subject, as confirmed by recital 46 of the GDPR.

In relation to employees' sensitive data, far stricter rules apply. Employers may lawfully process special categories of employee data only if the legal basis of art.9 par. 2b' (carrying out obligations in the field of employment, social security and social protection law), e' (processing of personal data made public by the data subject) or h' (processing for the purposes of preventive or occupational medicine, etc.) are met.

B. Transparency

Additionally, corporations and public authorities must be transparent regarding the measures they adopt, including the means and purpose of data collection. They must ensure that employees are aware of what data is being processed, why and with whom it is being shared in a way that is accurate, easily accessible and intelligible. Given the fact that the processing concerns sensitive data, a Data Protection Impact Assessment (DPIA) would be advisable.

C. Data Security

Any data processing in the context of mitigating the effects of COVID-19 must be carried out in a manner that ensures security of the data, in particular where sensitive data is involved. The identity of affected individuals should not be disclosed to any third parties or to their colleagues without a clear justification.

D. Data Minimisation

Pursuant to art.5 GDPR, only the minimum necessary amount of data should be processed by public authorities and companies, to achieve the purpose of implementing measures to prevent the spread of COVID-19.

E. Data Retention

Given the sensitivity of personal data, employers and public authorities should store data securely and for no longer than is necessary for the purpose for which it was processed. Businesses should aim to keep the retention period to a minimum whilst taking into account any local regulatory or legal requirements and the limitation periods for personal injury/health and safety claims.

III. Frequently asked questions regarding employment

- **Can an employer require employees to provide specific health information in the context of COVID-19?**

The processing of certain sensitive data that has been reported by employees, in relation to suspicion of infection, is permissible. Under national law, employers have a legal obligation to protect the health of their employees, while employees also have a duty to take reasonable care to protect their health and the health of any other person in the workplace. In this regard, employers would be justified in requiring employees to inform them if they have a medical diagnosis of COVID-19 in order to allow necessary steps to be taken. In all the above cases it is of the essence that the principles of data minimization security and transparency must are applied.

- **Is an employer allowed to perform medical check-ups on employees?**

Yes, under exceptional circumstances, measures such as the measurement of temperature, may be implemented, justified by the legal obligation of the employer to ensure that workers' health and safety are protected. The HDPA highlights, in this regard, that temperature measurement, given its intrusive nature, should constitute a measure of last resort, when all other appropriate measures cannot apply. Nonetheless, a systematic, constant and general collection of personal data, resulting in the creation and constant update of an “employee health profile”, would not easily be considered as being in accordance with the proportionality principle.

In any case, employers should ensure that all appropriate substantive and procedural safeguards are in place and provide information notice to data subjects about any planned processing. In addition, it is imperative that employers respect data subjects’ rights throughout the duration of such processing activities.

- **Can an employer disclose that an employee is infected with COVID-19 to his colleagues or to externals?**

In case of suspicion of infection, processing of specific employee’s data is permitted to the extent necessary to trail contacts and impose quarantine related measures. However, according to the HDPA, the disclosure of information on the health status of data subjects to third parties is not permissible, if lead to prejudice and stigmatization. Thus, the identity of affected individuals should not be disclosed to any third parties or to their colleagues without a clear justification. In this regard, employees should report an incident of infection, in a manner which does not anyhow identify, directly or indirectly, the affected person.

For more information visit the HDPA's website:

https://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=163,39,44,101,194,223,3,99

as well as the EDPB's website:

https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_el

Authors:

Angela Boletsi, Associate

Lucy Levi, Trainee Lawyer

Vasiliki Nikolaou, Trainee Lawyer

Anna Manda, Partner

Vassiliki Salaka, Partner