Practical guidelines for the lawful processing of personal data during the Covid-19 pandemic

Mastering the spread of so-called 'Coronavirus' is a major goal of governments and the public worldwide. In the meantime, the Coronavirus has already had significant and direct impact on the economic, social and, including, legal life of each country in a way we have not witnessed before.
While many laws and regulations have been enacted in order to deal with the pandemic in various spheres of the law, one that is not yet explicitly addressed by the supplementary legislation, but still relevant topic related to the health of individuals, remains the large-scale processing of personal data. In relation to the processing of personal data many open-ended questions arise in the current situation, which seek their answers.
Below you can find answers to the most frequently asked questions by clients and business partners of Penkov, Markov & Partners Law Firm related to the processing of personal data of employees, clients and third parties for the purposes of overcoming the Covid-19 pandemic.

What prohibits and allows GDPR?

General categories of personal data

The general provision of Art. 6 of the GDPR allows the processing of personal data (general categories such as names, address, telephone number, email address, etc.) on the basis of explicitly defined grounds - (i) legislative grounds; (ii) for the purposes of contract performance; (iii) provided consent; (iv) for the purposes of protection of vital interests, etc.

Special categories - incl. health condition

Article 9 of the GDPR prohibits the processing of so-called 'special categories' of personal data, including *data regarding the health of individuals*, with some exceptions: (i) *when an explicit consent is provided*; (ii) *for fulfillment of obligations arising from employment legislation*, etc.
We pay attention to this specificity since even measuring the temperature, for example at the entrance of a business or office, represents processing of a "special category" of personal data - related to the health condition.

In a PANDEMIC

In the case of Covid-19 where organizations/companies must comply with explicit instructions from public authorities; the World Health Organization and others, **there is a possibility to process special categories of personal data** (related to health status, biometric data, etc.) **on the grounds of Art. 9 (2), (I) of the GDPR**. In this case, the processing of the special categories of personal data would be necessary for reasons related to the public interest protection in

the field of public health, including the protection against serious cross-border health threats, etc.

In addition, point 46 of the GDPR Preamble states that the processing of personal data should be considered **lawful where necessary in order to protect the interest of prime importance for the lives of individuals. This is exactly the current situation on a global scale.** Some types of processing can serve both important areas of public interest and the vital interests of the data subject, for example *"when processing is necessary for humanitarian purposes, including epidemic surveillance and countering their spread or in emergency humanitarian situations, in particular in the case of natural or man-made disasters. "*

Regarding the employers, the Bulgarian legislation, and in particular the Labor Code sets an obligation for ensuring of healthy and safe working conditions for the employees. As part of these measures the employers could collect information on the health of employees related to the particular illness and in accordance with the National Crisis Staff instructions. **On the grounds indicated above**, **any such processing could be carried out in the context of the current situation and without the explicit additional consent of the employees.** The stated **obligation for the employers** as well as **the provision of Art. 9 (2), (I) of the GDPR,** interpreted in their entirety and connection, **provide grounds for lawful processing of special categories of personal data during a pandemic situations.**

Processing after ensuring of technical and organizational measures

Notwithstanding the above, it should be remembered that the GDPR imposes a number of obligations and restrictions with a view to providing technical and organizational measures to protect the processed personal data, irrespective of the processing grounds. The aforementioned measures should be taken in advance, i.e. before processing and shall be applied strictly.
In this sense, the obligations of confidentiality, data encryption, anonymization or pseudonymization (where possible), restriction of access and many others remain in force and companies, organizations, public authorities and all other data controllers should comply with them.

Is it possible for an employer to require its employees, customers and visitors to complete a questionnaire containing current travel information in countries affected by the virus, as well as medical information, including: fever symptoms, body aches, etc.? Is it possible for an employer to measure the body temperature of their employees, customers, office visitors, etc.?

Companies/organizations have the legal ability to ask their employees, customers, visitors for information about their health status, but only if this

information relates to symptoms arising prior to Covid-19 infection, e.g. high body temperature, cough, body aches and fever symptoms.
It is good European practice the processed information to be pseudonymized and stored in files with coded/encrypted names that cannot be linked to a specific individual in case of unauthorized external access.
The most appropriate and secure approach that employers can take, both for their employees and visitors, customers and more, is to collect the abovementioned information through anonymous questionnaires (i.e. anonymized), including temperature measurement without linking the result to an individual.
Thus, the assessment of whether an individual should have access to the company/organization would be performed at the moment in which the individual is about to enter without necessity for processing of personal data regarding his condition, body temperature, etc. within the meaning of GDPR. In this case, there will also be no need to store the information collected unless the company/organization aims to use it for statistical purposes.

For what periods could be stored the collected personal data?

The Personal Data Protection Act and the GDPR do not contain specific time limits for the storage of special categories of personal data processed for the purposes listed above.
The information provided should be kept for short periods of time, e.g. 30 days or until the pandemic has passed, according to the goals set for processing and using the information. Of course, in case of explicit instructions from the Crisis Staff or in the event of a legal change, this should be taken into account.
After the expiry of the specified storage periods, the data must be destroyed and, where necessary, including when there is a legal basis, the information may be updated and collected again by individuals.

What data protection measures should be undertaken?

Companies/organizations should adhere to the basic principles of lawful processing of personal data set out in the GDPR, e.g. proportionality, data minimization, transparency, etc.
In this regard:

- It shall be determined the premises, software, etc. where personal data will be stored;
- It shall be designated a person (or several, depending on the scale of the processing), responsible for complying with the lawfulness of the processing, including ensuring access to the data when necessary, timely destruction of the data after the expiration of the storage period, etc.
- The persons whose personal data will be processed shall be notified in this regard;
- When possible – the data shall be encrypted, pseudonymized, even anonymized etc.

It is important to note that the general obligations related to reporting of data security breaches (up to 72 hours after the breach is found), sending replies to requests from data subjects, etc. should be followed as before.

Is it possible an information about confirmed cases of Covid-19 to be shared with third parties?

This issue should be examined on a case-by-case basis from the perspective of the specific third parties to whom the information will be provided.
However, this type of information should be provided to public authorities and health authorities which would help to deal with and reduce the pandemic, including in connection with the mandatory 14-day quarantine of sick persons. In the current situation, if the employee visited their workplace during the quarantine period, in order to protect the public interest and the lives and health of other employees, the health authorities may find it necessary to quarantine all other employees and the work premises.

Sharing information on confirmed Covid-19 cases with other employees should be avoided, and it should only be possible if absolutely necessary to assess whether other employees have been in contact with the individual and, accordingly, have been infected. Taking into account the circumstances, appropriate approach would be communication the information anonymously - without identifying the particular individual.

This Information Legal Bulletin provides general information related to the processing of personal data during the Covid-19 pandemic. It is not exhaustive and is an interpretation of the legal rules and practices of regulatory authorities in the European Union by the Data Protection Team at Penkov, Markov & Partners Law Firm.

With respect to other current topics, in relation to the legislation, stipulating the relationships at the state of emergency, you may find information on our website – www.penkov-markov.eu. Of course, you may address us for any additional information and assistance at lawyers@penkov-markov.eu.