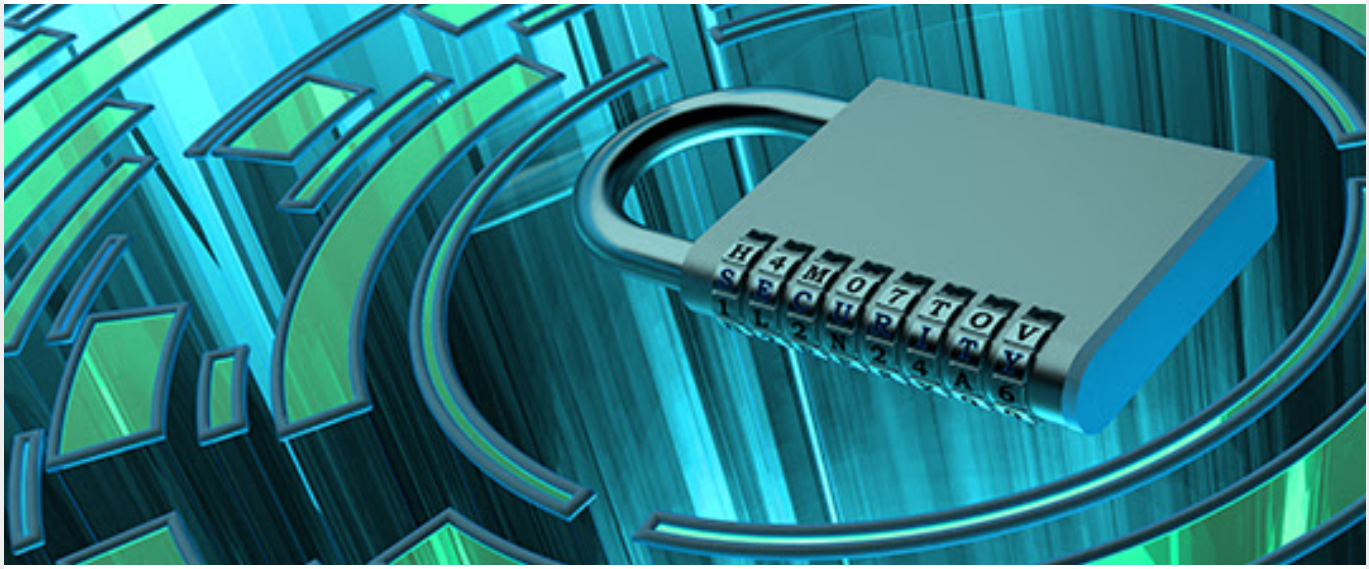
Turkey | Data protection during the COVID-19 pandemic

April 2020



Dear Clients, Colleagues and Friends,

Following the announcement of the COVID-19 pandemic by the World Health Organization, increasingly restrictive measures to curb the spread of the virus have been taken in Turkey, as in many other countries all over the world. These measures lead to additional personal data processing activities, and raise new challenges in terms of compliance with data protection law.

The Turkish Data Protection Authority (the "**DPA**") has released two announcements on 23 March 2020 and 27 March 2020 regarding the data processing principles to be taken into account during the fight against the pandemic, including a set of Frequently Asked Questions, and underscored the data security obligations of data controllers and data processors in this context.

It is important to point out that the measures implemented to fight the pandemic do not abolish or suspend the current obligations of data controllers arising from Law no. 6698 on the Protection of Personal Data (the "**Law**"). Data controllers and data processors must ensure that data processing activities carried out within the scope of these measures remain in compliance with the Law, and should take all the necessary administrative and technical measures to protect the data they process under unauthorised access or use.

The DPA's announcements emphasise that it is crucial for data controllers to pay attention to the following principles when processing personal data, especially health data:

Fundamental principles: Data processing activities within the scope of the measures taken against the pandemic should be implemented in accordance with the fundamental principles of compliance with the law and good faith principles, the obligation to keep data accurate and up-to-date (when necessary), and the obligation only to process personal data for specific, clear and legitimate purposes and to keep the process

relevant, limited and proportional to such purposes. Personal data should only be stored for the period provided under the law or for the period needed to achieve the data processing purpose. If the reasons for processing no longer exist, the personal data being processed must be deleted, destroyed or anonymised.

Compliance with law: The conditions for lawful processing of personal data are set forth under Article 5 of the Law, while Article 6 addresses the conditions applicable to special categories of personal data, which include health data. Personal data processing activities undertaken within the scope of the fight against the pandemic must remain compliant with these conditions.

If the health data of employees is processed without their explicit consent, the processing must be carried out by the workplace medical doctors, who are subject to a duty of confidentiality. In addition, the measures set forth in Decision no. 2018/10 dated 31 January 2018 of the Turkish Data Protection Board (additional measures to be adopted for special categories of personal data) must be put in place.

Information obligation: Data controllers must fulfil their information obligation during the pandemic as well. The data subjects should in particular be informed of how their data will be processed, including the purpose for which their data is collected and the time period for which it will be stored.

Privacy: Administrative and technical measures should be implemented to ensure the security of the personal data to be processed within the scope of the measures taken against the pandemic. The personal data of persons affected by the disease should not be disclosed to any third party without a clear and mandatory reason. It should also be kept in mind that the illegal posting of personal data, especially health data, on social media accounts and similar platforms constitutes a crime under the Turkish Criminal Code no. 5237.

Data minimisation: As for all data processing activities, data processing carried out for the purpose of preventing the spread of the Covid-19 virus should remain consistent with and limited to the purpose of processing. The processing of any data in excess of the necessary data must be avoided.

All the measures announced by public authorities and institutions such as the Ministry of Health, the Ministry of Industry and Technology, the Ministry of Family Affairs, and Labour and Social Services should be applied in accordance with the principles set out above. This includes such steps as measuring the fever of employees, or obtaining declarations from employees in case of contact with persons who have travelled abroad in the past 14 days or were diagnosed with the disease.

Frequently Asked Questions

What kind of security measures should be taken in the context of remote working?

As the remote working model has become more widespread in the recent period, administrative and technical measures should be taken against the risks that remote working conditions pose to data security. In order to minimise these risks, it should in particular be ensured that the data traffic between the systems is conducted with secure communication protocols, that there is no vulnerability in the system, that the anti-virus programs and firewalls are up-to-date, and that employee awareness on the security of personal data is increased. Data controllers must keep in mind that the measures taken to fight the pandemic do not abolish or suspend their obligation to ensure the security of personal data arising from the Law.

Can the employer disclose that an employee is carrying the virus to other employees?

The employer has a duty to implement the necessary measures in the workplace to comply with its obligations under occupational health and safety regulations, and should thus inform other employees if an employee is affected by the disease. While doing so, however, the employer should not provide more information than necessary, such as disclosing the identity of the concerned employee. It is possible for the employer to indicate

that an employee has been infected and will work from home or be on leave. Unless necessary for the purpose of implementing precautionary measures, however, details that can indicate the identity of the employee, such as the employee's name, level or team, should not be disclosed.

Can the employer request from all employees and visitors information as to whether they have symptoms of Covid-19 (fever, difficulty in breathing, etc.) or if they have recently travelled to countries that are affected by the pandemic?

Within the scope of its obligation to protect the health of its employees under occupational health and safety regulations, the employer can request such information from employees and visitors, but the request must be measured and proportionate. In this context, not all the processed data will be special categories of personal data. Where the data is not sensitive data (such as the country of travel), the processing conditions set forth under Article 5 of the Law will apply.

Can the employer share the health information of the employees with the authorities?

In accordance with applicable regulations on infectious diseases, the employer may share the personal data of infected persons with the relevant authorities.

Are the periods under the Law and related legislation for the data controller to respond to the applications of the data subjects and to the DPA still valid?

The legal periods under the law and related legislation are not extended, and it is important to comply with these periods. The DPA however indicated that the extraordinary circumstances caused by the pandemic will be taken into consideration while enforcing the 30-day period to respond to data subject applications and the 72-hour period to notify a data breach.

Contact Us

Stéphanie Beghe Sönmez
Partner
sbeghe@paksoy.av.tr

Neslihan Kasap
Associate
nkasap@paksoy.av.tr