Client Alert | Data, Privacy & Cybersecurity

COVID-19 and Data Protection Compliance in Turkey

April 24, 2020

Authors: **Selin Kaledelen, Damla Çay, Ebubekir Bal**

Following the outbreak of COVID-19 and its development into a global pandemic, organizations have been implementing exceptional measures to safeguard the health of employees, customers and others. Organizations are also endeavouring to maintain 'business-as-usual' to the extent allowed by their particular circumstances.

As part of White & Case's ongoing legal updates on COVID-19-related issues affecting our clients' businesses around the world,[1] this article discusses the resulting data protection compliance obligations under Turkish law, based on guidance and principles provided and measures taken by the Turkish Personal Data Protection Authority regarding COVID-19, and requirements to be fulfilled in respect of the Turkish Personal Data Protection Law numbered 6698 and its secondary legislation.

Existing obligations continue to apply during the COVID-19 outbreak

Data controllers' and processors' obligations arising from the PDPL continue to apply. Without an amendment to the existing legislation, data processing activities should take place within the boundaries drawn by current data privacy legislation.

The PDPL and the Authority

The Turkish Personal Data Protection Law numbered 6698 ("the PDPL") is the first comprehensive legislation concerning personal data protection in Turkey. The PDPL was adopted by the Grand National Assembly of Turkey on March 24, 2016, came into force in the same year, and continues to apply.. The PDPL uses EU Directive 95/46/EC as its basis and contains largely similar provisions.

The Turkish Personal Data Protection Authority ("the Authority") has been officially active since January 30, 2017. The Personal Data Protection Board (the "**Board**") is the decision-making body of the Authority.

The PDPL does not apply to the data processing activities of public institutions

[1] For further information, please visit the White & Case Coronavirus Resource Center.

The Authority recently published guidelines on personal data processing activities during the COVID-19 pandemic.

The Authority reiterated the processing rules set by the PDPL. Briefly, the Authority has underlined:

- the general principles of compliance with the laws and good faith, purpose and storage limitation, proportionality, accuracy and integrity;
- the obligation to inform, transparency;
- data minimization; and
- confidentiality and the importance of implementing the necessary technical and administrative measures to ensure the security of personal data while processing personal data.

The Authority noted that the PDPL does not apply to the data processing activities of public institutions or organizations authorized and appointed by law for establishing public security and public order, pursuant to the exceptions set forth under Article 28(1)(ç) of the PDPL. Thus, it considers the measures against COVID-19 as a public security and public order matter.

For private institutions, the Authority highlighted that the legal grounds for the processing of personal data and the special categories of personal data ("**SCD**") as provided under Articles 5[2] and 6[3] of the PDPL must be in place. It also referred to the Board's decision dated January 31, 2018 and numbered 2018/10, titled "**Adequate Measures to be taken by the Data Controllers for Processing of Special Categories of Personal Data**" to draw attention to the specific security measures provided for SCD.

It is notable that the Authority preserves its strict position regarding the cross-border transfer of personal data. While most remote training software uses cloud services for which the servers are based outside Turkey, it announced that the requirements of Article 9 of the PDPL regarding cross-border data transfer continue to apply.

Controversial Legal Framework for Processing Health Data

The processing of health data has always given rise to legal problems under Turkish law. Pursuant to the PDPL, health data is considered to be SCD, and is subject to stricter data processing requirements and greater protection.

As a rule, SCD can only be processed if the data subject's explicit consent is obtained. While other SCD (such as the person's race, ethnicity, religion, etc.) may be processed without the data subject's explicit consent when allowed by law, health data can only be processed without explicit consent:

---

[2] **Conditions for processing personal data**
ARTICLE 5 – (1) Personal data shall not be processed without explicit consent of the data subject.
(2) Personal data may be processed without seeking the explicit consent of the data subject only in cases where one of the following conditions is met:
a) It is expressly provided for by law.
b) It is necessary for the protection of the life or physical integrity of the person himself/herself or of any other person, who is unable to give his/her consent due to physical disability or whose consent is not deemed legally valid.
c) Processing of personal data of the parties to a contract is necessary, provided that it is directly related to the establishment or performance of the contract.
ç) It is necessary for compliance with a legal obligation to which the data controller is subject.
d) Personal data have been made public by the data subject himself/herself.
e) Data processing is necessary for the establishment, exercise or protection of any right.
f) Processing of data is necessary for the legitimate interests pursued by the data controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

[3] **Conditions for processing of special categories of personal data**
Article 6 - (1) Personal data relating to the race, ethnic origin, political opinion, philosophical beliefs, religion, religious or other belief, appearance, membership in associations, foundations or trade unions, data concerning health, sexual life, criminal convictions and security measures, and biometric and genetic data are deemed to be special categories of personal data.
(2) It is prohibited to process special categories of personal data without the explicit consent of the data subject.
(3) Personal data, except for data concerning health and sexual life, listed in the first paragraph may be processed without seeking explicit consent from the data subject, in the cases provided for by law. Personal data concerning health and sexual life may only be processed, without seeking explicit consent from the data subject, by persons under the obligation of confidentiality or authorized public institutions and organizations, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of healthcare services, as well as their financing.
(4) Adequate measures determined by the Board shall also be taken while processing the special categories of personal data.

- for the purposes of protection of public health, preventive medicine, medical diagnosis, treatment and healthcare services, planning and management of health services or their funding; and
- by persons under the obligation of confidentiality[4] or authorized institutions and organizations.

Hence, the PDPL largely limits both the persons who may process health data and the purposes for which it can be processed. Personal health data cannot be processed without explicit consent by persons not authorized under this Article, even if the purpose for which it would be processed is provided for by the law. As explicit consent can always be withdrawn, the processing of personal health data by employers is very problematic.

Article 8 of the PDPL provides that, as a rule, personal data cannot be transferred without the explicit consent of the data subject. One exception to this rule is the data transfer requirements under other laws. Pursuant to Public Health Law Numbered 1593 (the "**Public Health Law**"), certain institutions and businesses, such as hospitals, schools, factories, production facilities, charity institutions, shops, hotels and other accommodation providers (*who are not considered as persons under the confidentiality obligation*) are obliged to report any person infected with epidemical diseases enumerated under Article 57 and other epidemics to be determined by the health authorities to the relevant authorities. Although this old law dated 1930 does not specify COVID-19 among these epidemical diseases, the Public Health Law is an example of the legal requirement exception to the personal data transfers. However, personal data transfer is also a data processing activity. The contradiction between Article 6 of the PDPL extremely limiting the processing of health data, and the data transfer requirements provided by other laws, is clear.

The secondary legislation on the processing of health data has also been problematic. In this respect, the Ministry of Health published the Regulation on the Processing and Privacy of the Personal Health Data in the Official Gazette dated October 20, 2016 numbered 29863 (the "**Former Health Data Regulation**"), shortly after the adoption of the PDPL. However, the enforcement of the Former Health Data Regulation was suspended on July 6, 2017 with the Council of State stating that the Former Health Data Regulation had been prepared without obtaining the Authority's opinion. Although an amendment was made to the Former Health Data Regulation following the Council of State's suspension of the enforcement decision, the Former Regulation was suspended by the Council of State again on October 9, 2018. After three years of ambiguity, the Former Health Data Regulation was abolished, and the Regulation on Personal Health Data published in the Official Gazette dated June 21, 2019 and numbered 30808 (the "**Regulation on Personal Health Data**") entered into force. With respect to data processing transfer of health data, the Regulation on Personal Health Data refers to general rules for data transfer set forth under the PDPL and the problems arising from this remain unsolved.

In Respect of Mobile Data

The Ministry of Health developed a project named "*Pandemic Isolation Tracking Project*" in order to fight the spread of the virus. According to the website of the Directorate of Communications, the aim of the project is to ensure isolation of those diagnosed with COVID-19 and those who are in contact with them. The project has been implemented in cooperation with the Ministry of Health, Information and Communication Technologies Authority and all GSM operators. Within the scope of the project, data from GSM operators will be used to track whether or not positive cases comply with the isolation rule. If those subject to self-isolation due to the risk of COVID-19 leave their homes, they will receive a warning message on their phones, and an automatic call asking them to return to their place of isolation. Should they fail to comply with such warning, relevant law enforcement units will be informed and relevant administrative measures and sanctions will be imposed.

The Authority announced on its website that there is no obstacle to the processing of location data by public institutions and organizations in order to prevent the spread of the disease as explained above, as this kind of processing falls within the scope of exception provided under Article 28 of the PDPL. The Authority nonetheless highlighted the importance of taking all technical and administrative measures to ensure the protection of such personal data and deletion of such data when the conditions no longer require the processing of such data.

[4] According to the Authority, such person may be, for example, the occupational doctor.

Brief Guide for Employers

In its public announcement dated March 27, 2020, the Authority also published a FAQ for employers:

- **Remote working**: The employees' use of their own devices or security measures taken by the employees while working remotely do not release data controllers from their obligation to take necessary technical and administrative measures to ensure the security of personal data. In order to minimize the risks that may be caused by remote working, all employees must be diligently informed about data security and all necessary measures must be taken. This particularly applies to the flow of data traffic between systems through secure communication protocols - these systems must not contain any weaknesses and/or vulnerability and anti-virus systems and firewalls should be kept up to date.

- **Disclosure of employees' health data:** Employers must inform other employees about COVID-19 cases in the company. Unless absolutely necessary, such briefings must not include the names or other identifiers of the infected employee. Unnecessary information should not be provided and, if the disclosure is deemed necessary, the relevant employee should be informed about such disclosure beforehand.[5] The employers may share the personal data of the infected persons with the relevant authorities pursuant to Article 8 of the PDPL and other public health laws.

- **Collection of health and travel history data from employees and visitors:** The Authority stated that employers are under a duty to protect occupational health and to provide a safe working environment. Therefore, employers have legal grounds to request information from their employees and visitors as to whether they have visited infected areas and/or whether they have any symptoms. This information request must be necessary and proportionate and have a strong justification based on risk assessment (such as the presence of high-risk groups in the relevant company).

Final Notes

The Authority has decided not to accept data subject complaints, data breach notifications and Data Controllers' Registry ("**VERBIS**") application forms delivered by hand during the outbreak. Instead, it announced that:

- data subject complaints should be made via mail, cargo or the complaint module present on the Authority's website;

- data breach notifications should be made via e-mail or the module provided on the Authority's website; and

- VERBIS application forms should be transmitted via mail, cargo or registered electronic mail.

Furthermore, the Authority also announced that, considering the different operational practices (remote work, alternate work, etc.) conducted by data controllers during the pandemic, the Board will take these extraordinary circumstances into account in the evaluation of the periods that data controllers are obliged to comply with for application forms or data breach notifications, although their compliance obligations are still valid.

GKC Partners

Ferko Signature

Büyükdere Cad. No: 175 Kat: 10

Levent 34394 Turkey

T + 90 212 355 1300

[5] The example notice provided by the Authority is as follows: *"We would like to inform you that one of our colleagues working on the fifth floor of our head office tested positive for COVID-19. We will inform the individuals who might have had contact with our colleague by considering the dates during which the person who has tested positive was at the office."*