Roads to Digital Resilience with COVID-19: Data Privacy Perspective

Authors: Gönenç Gürkaynak, Esq., Ceren Yıldız, Burak Yeşilaltay, Elifcan Çepoğlu and Ezgi Pamukçu, ELIG Gürkaynak Attorneys-at-Law

I. COVID-19 Reality

Getting ready to claim its spot in the history books, COVID-19 has been spreading all around the globe at a drastic pace and highlighting the need for the international community to develop a system of emergent healthcare support to cope with disease outbreaks.

This wave of virus has inevitably moved most nations toward a new realm wherein governments have shut down borders and imposed quarantines and companies have adopted work-from-home policies to encourage workers to stay at home. Change in the settings, rules, conditions emerged as a result of these implemented emergency measures may lead to data privacy concerns as these measures are likely to involve processing of personal data particularly health data, and thus may give rise to data protection law related compliance issues and data breaches.

II. Data Concerning COVID-19 under Turkish Legislation

A resurgence of personal data processing is being experienced due to or for the measures taken within the scope of COVID-19 by data controllers, public authorities and private companies.

As any information that relates to an identified or identifiable individual, data concerning COVID-19 is likely to include personal data of people who have symptoms or who have possibly contracted the virus and have tested either negative or positive as well as data of employees who were encouraged to work from home for isolation. In addition to this, travel information or visitors may also be within the scope of personal data. However out of all these personal data, data concerning health is likely to be most sensitive type of data to be dealt with under COVID-19 outbreaks.

Data concerning health refers to the physical or psychological health of a real person, or the health service provided to such person, including data which reveals information about health status and as similar to the GDPR rules, falls under the special categories of personal data under Law No. 6698 on Personal Data Protection Law (“DPL”).

1. Health Data under the DPL

Pursuant to Article 6 of DPL data concerning racial or ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and clothing, association, foundation or trade-union membership, health or sex life, and criminal conviction and security measures regarding a person along with their biometric and genetic information are *special categories of personal data*.

Accordingly, *health information* is considered within the scope of special categories of personal data, which refers to physical and psychological health of an identified or identifiable real person and information relating to the health services provided to that person.

2. Health Data Regulation

Health data security has become one of the most important aspects of data protection, and in addition to health data provisions covered under the DPL, the Regulation on Personal Health Data ("Health Data Regulation"), enacted by the Ministry of Health particularly addresses the principles and procedures to be followed in this regard as a secondary legislation.

Although there is no specific set of rules enacted regarding pandemics such as COVID-19, general rules set out in the DPL and the Health Data Regulation will also be applicable to date retained due to COVID-19 outbreak. In order to prevent unlawful access to personal data, Health Data Regulation limits access to data to only required and authorized healthcare personnel. Pursuant to Article 6 of the Health Data Regulation, authorized personnel may access personal data, provided that the relevant access is within the scope of the health services offered to patient.

Furthermore, in order to foster and encourage research, scientific knowledge and innovation, Health Data Regulation allows scientific studies on health data, and this might be applicable to COVID-19 patients. For personal data to be utilized in such studies, data should be anonymized with official statistics for the purposes of research, planning or statistical operations. Moreover, Health Data Regulation authorizes use of personal health data for artistic, historical, literary or scientific purposes or within the scope of freedom of speech; provided that national defense, national security, public safety, public order, economical safety, privacy of private life or personal rights are not violated and the processing of data does not constitute a crime.

III. Processing Conditions

To the extent that the data identifies or may identify an individual, processing such data could either be based on the explicit consent of the data subject or other legal grounds under which the processing falls under. With regards to the health data, the processing conditions are more limited.

Per DPL, health data may be processed without the explicit consent of the data subject, if the data is processed by authorized entities and institutions or by persons who are under the confidentiality obligation for the purposes of protection of public health, preventive medicine, medical diagnosis, planning, managing and financing of treatment and maintenance services (Article 6/3 of DPL).

In light of the foregoing rule, data controller (e.g. *the employer*) may process data subject's (e.g. *the employee*) health data (e.g. *whether an employee has been tested positive*) through the authorized persons under the confidentiality obligation (e.g. *workplace doctor*) to combat the Corona virus within the scope of public health, without his/her explicit consent.

Furthermore, due to their nature, processing health data would also require adequate data security measures to be taken, as determined by Turkish Data Protection Authority ("DPA") in its decision with number 2018/10[1].

Having said that, there is no such rule that all the data relating to COVID-19 related issues would constitute special categories of personal data. For instance, data relation to an individual's travel records might not be deemed special categories of personal data, unless that could reveal an indication of a possible medical condition, and thus, could be evaluated in light of Article 5/2 rather than Article 6/3 of DPL.

IV. General Exemption Rule: Article 28 of DPL

Article 28 of the DPL provides general exemptions for certain and limited cases and states that DPL does not apply if one of the conditions provided therein exists.

In accordance with the relevant provision, DPL is not applicable if personal data is processed for national defense, national security, public safety, public order or economical safety and by public institutions and organizations which are authorized by law within the scope of their preventive, protective and intelligence activities (Article 28/1(ç) of DPL). The public order can be defined as ensuring the safety, health and wellness of individuals' daily lives and extends to the public health either. However, as the provision reads itself, this exemption should be solely applicable for public institutions and organizations or their employees.

For instance, in a case where people are under quarantine due to the risk of an epidemic disease such as COVID-19, the government might process people's location data in order to prevent them from leaving the quarantine zone; since there is a superior public interest in this case. However, an employer might not process employee's location data without being subject to the DPL. That said, an employer may transfer personal data to one of these authorized public institutions or organizations upon a duly sent request in accordance with the laws, due to the necessities of COVID-19 within the scope of his/her legal obligation, to the extent required.

Another exemption from the DPL is processing personal data for artistic, historical, literary or scientific purposes or in the scope of freedom of speech, provided that national defense, national security, public safety, public order, economic safety, privacy or personal rights are not violated and that the data processing does not constitute a crime (Article 28/1(c) of DPL). Therefore, even though the "scientific purposes" should also comprise the cases where data relation to COVID-19 are processed, one might argue that this provision targets health or research institutions' processing activities to gather detailed findings and knowledge on COVID-19, to update databases and conduct studies.

[1] DPA's decision (with number 2018/10) on the adequate measures was published in the Official Gazette on March 7, 2018. DPA indicated in its decision that data controllers should determine a separate, systematic, and manageable procedure with definite rules for the protection of special categories of personal data. The decision also requires data controllers (i) to take certain measures regarding its personnel who deal with special categories of personal data, such as providing them with periodic trainings on the legislation, requiring them to sign non-disclosure agreements and determining the scope and limits of their authorizations, checking their authorizations periodically, ensuring the return of inventory that was furnished to authorized personnel after a change of their position/duty or at the end of their employment, and (ii) to adopt certain security measures for safeguarding such data in physical and electronic environments. The decision also provides specific procedures that must be followed by data controllers for the transfer of special categories of personal data (For more detailed information, see our Mondaq article Personal Data Protection Board's Decision On Adequate Measures To Be Taken By Data Controllers Regarding Special Categories Of Personal Data).

V. Other Points to Note

Other than the points explained above, data controllers should also take into consideration other steps to ensure their compliance with their data privacy obligations. In that regard, we recommend that data controllers should pay attention to the following aspects:

- ***Seeking alternative methods instead of processing health data***: Turkish data protection legislation does not provide specific rules for processing special categories of personal data without explicit consent in terms of data controllers (which do not fall within the scope of authorized public bodies), even in quite exceptional cases. Furthermore, the DPA has not published a guideline on this particular matter yet. Therefore, we recommend that data controllers proceed with other information without processing special categories of personal data to the extent possible. While doing this evaluation, data controllers should always ask the question "whether is it strictly necessary to process health data?". If the answer is no, then they should proceed with the alternative method, to be on the safe side.

- ***Privacy notices:*** Whether the data processed constitutes personal data or special categories of personal data, data controllers should maintain their obligation to inform data subjects and update their informatory notices in a way to cover personal data processing activities to be conducted within the scope of COVID-19. Data controllers should be clear, explain the reasons and purposes of such collection and inform data subjects about their rights, as required under DPL.

- ***Always remember general principles:*** For all types of personal data, data controllers should always bear in mind the general principles of the DPL. Personal data must be (i) processed lawfully and fairly, (ii) accurate and where necessary kept up to date, (iii) processed for specified, explicit and legitimate purposes, (iv) relevant, limited and not excessive in relation to the purposes for which they are processed, (v) kept for as long as it is foreseen by relevant legislation or it is necessary for the purposes of processing.

- ***Erase, destroy or anonymize data:*** In the event that the personal data collected are no longer required, data controllers should erase, destroy or anonymize the personal data. Similarly, data controllers should not retain personal data for longer than the purposes of collection and longer than the periods allowed by laws.

- ***Adopt authorization and control matrix:*** Access to the systems that contain personal data should also be restricted, as these systems may also include sensitive data about individuals and may be open to threat while working remotely through the COVID-19 threat. In that regard, employees should have access authorization to the extent that it is required for their authorities and responsibilities and they should access to the relevant systems through user names and passwords.

In addition to the foregoing, data controllers should also implement a number of supplementary measures that are controlled on a regular basis within the scope of several principles (e.g. a well-structured firewall and gateway, encouraging employees to lock screens when away, secure home routers and remote access systems, keeping regular logs, creating an

official reporting procedure for employees' to report security gaps or threats etc.) to ensure security of personal data.

VI. DPA's Recent Announcements on COVID -19

Even though there are no specific data protection guidelines proposed by DPA in relation to COVID-19 outbreak, through its recent announcements, the DPA has expressed its position with regard to review of requests concerning the privacy issues.

1. DPA's announcement on conveying complaints, breach notifications or VERBIS application forms

On March 18, 2020, DPA has published an announcement regarding conveying (i) complaints, (ii) data breaches or (iii) VERBIS application forms electronically or through mail or cargo, to prevent possible spread of COVID-19.

In that regard, instead of conveying these forms in hand, DPA recommends data controllers to convey (i) complaint applications via mail, cargo or through https://sikayet.kvkk.gov.tr/ , (ii) data breach notifications through e-mail messages at ihlalbildirimi@kvkk.gov.tr or through https://ihlalbildirim.kvkk.gov.tr/ and (iii) VERBIS application forms via mail, cargo or KEP address.

2. DPA's announcement on timelines for complaint and breach notification proceedings

On March 23, 2020 DPA has announced that although it is important to comply with the periods indicated under DPL, all data violation notifications submitted to DPA within the scope of the personal data protection legislation will be reviewed by taking into consideration today's complusory operational practices (remote work, alternate work, etc.) and thus each application will be observed accordingly given the extraordinary conditions of today's environment.

VII. Conclusion

As the entire globe has been facing with a common challenge of COVID-19, a sudden shift has taken place with regard to health and data dynamics. COVID-19 has become the sole subject discussed by all news channels, governmental bodies, public and private personalities of every nation as a non-negligible crises. Since majority of sectors will be affected by measures taken in response to the outbreak of the coronavirus disease proactive security measures are being implemented. Ultimately this global siege will come to an end, but adopting rapid rules and measures around data protection to mitigate such privacy and cyber security risks would allow avoiding or mitigating potential legal issues in the aftermath of this crisis.

Article contact: Gönenç Gürkaynak, Esq. Email: gonenc.gurkaynak@elig.com

(*First published by Mondaq on March 27, 2020*)