Bioethica

Vol 8, No 1 (2022)

Bioethica

Protection of medical data within the scope of the Law on Protection of Personal Data

Özge Dirim Çiftçi

doi: 10.12681/bioeth.30544

To cite this article:

Çiftçi, Özge D. (2022). Protection of medical data within the scope of the Law on Protection of Personal Data. *Bioethica*, *8*(1), 66–73. https://doi.org/10.12681/bioeth.30544

Protection of medical data within the scope of the Law on Protection of Personal Data

Özge Dirim Çiftçi

Stagiaire, Hellenic National Commission for Bioethics & Technoethics

ozgedciftci@gmail.com

Abstract

As a result of non-stop developing technology, each corner of our lives become more and more reachable. Although privacy has always been very valuable and modern laws has taken steps to provide security of privacy, nowadays it takes only some seconds to reach the surname, workplace, the address etc of a person; even of a family. Although some may believe sharing information is harmless, from spam emails to obsessive stalking there is not an actual limit of what can be done with wrongly accessed personal data.

When having frequent commercial calls from firms or missing your important mails because of the commercials that fill your mail box, we experience that even the slightest privacy violation can be very annoying. However some personal data are exactly what people face discrimination of. In todays world it is common to see people are discriminated due to their religion, sexuality, politic views, past convictions and even due to their health conditions. The results of discriminations may vary from not being included to social life to mobbing at work; in some extreme cases it may even put the persons life at risk by making them a target. Considering the possible risks and the easiness to reach, as technology has been developing constantly, the need for data protection is more visible than ever. This article aims to explain the protection of medical data in Turkish Legislation by focusing on Law on Protection of Personal Data.

Keywords: personal data, medical data, Law on Protection of Personal Data, Personal Data Protection Board.

Η προστασία των ιατρικών δεδομένων εντός του πεδίου εφαρμογής του (τούρκικου) νόμου για την προστασία δεδομένων προσωπικού χαρακτήρα

Özge Dirim Çiftçi

Ασκούμενη, Εθνική Επιτροπή Βιοηθικής & Τεχνοηθικής

Περίληψη

Αν και επικρατεί η εντύπωση ότι η κοινή χρήση προσωπικών πληροφοριών είναι αβλαβής, δεν υπάρχει πραγματικό όριο για τις συνέπειες της χρήσης δεδομένων, η πρόσβαση στα οποία δεν έχει ελεγχθεί. Λαμβάνοντας υπόψη τους πιθανούς κινδύνους και την ευκολία πρόσβασης, καθώς η τεχνολογία αναπτύσσεται συνεχώς, η ανάγκη για προστασία δεδομένων είναι πιο ορατή από ποτέ. Αυτό το άρθρο στοχεύει να εξηγήσει την προστασία των ιατρικών δεδομένων στην τουρκική νομοθεσία, εστιάζοντας στον νόμο για την προστασία των προσωπικών δεδομένων.

Λέξεις κλειδιά: προσωπικά δεδομένα, ιατρικά δεδομένα, (τουρκικός) νόμος για την προστασία δεδομένων προσωπικού χαρακτήρα, (τουρκική) επιτροπή για την προστασία προσωπικών δεδομένων.

1. DATA PROTECTION LEGISLATION OF TURKEY

Until 7th April 2016, except for some certain sectors, data protection in Turkey was limited with very few provisions in Constitution of Turkey[1] and in Turkish Penal Code[2]; providing very limited protection of the personal data by provisions limited to certain cases followed by long and complex trial processes.

1.1. The Constitution

The Constitution regulates obligations as well as protecting rights of the citizens. The protection of the personal data is regulated in Constitution of Turkey by basic provisions.

Article 20 – *Everyone has the right to demand respect for their private and family life. Confidentiality of private life and family life is inviolable.*

As an annex to the article 20, in 2010 a provision regulating specifically protection of personal data was added.

Additional Clause 7/5/2010- *Everyone has the right to demand the protection of their personal data. This right also includes being informed about the personal data about the person, accessing these data, requesting their correction or deletion and learning whether they are used for their purposes. Personal data can only be processed in cases stipulated by law or with the explicit consent of the person. The principles and procedures regarding the protection of personal data are regulated by law.*

1.2. Turkish Criminal Code

Turkish Criminal Code(here after the TCC) regulates data protection to a very limited extent; mainly the consequences of wrongful usage of personal data such as violating privacy. The relevant acticles are as the following:

Article 135- *(1) Anyone who unlawfully records personal data is sentenced to imprisonment from one year to three years.*
(2) Personal data such as political, philosophical or religious views, racial origins of the person; The penalty to be imposed in accordance with the first paragraph is increased by half, in case it unlawfully relates to their moral tendencies, sexual life, health status or union affiliations.
As seen in the article 135 of the TCC, in case of a violation of protection of sensitive personal data, such as data on health or religion, the penalty increases by half.

Article 137- *(1) The offenses defined in the above articles;*
a) If commited by a public official and by misuse of his/her duty or,
b) If committed by taking advantage of the convenience provided by a certain profession and art, the penalty to be imposed is increased by half.
Article 138- *(1) Those who are obliged to destroy the data within the system despite the expiry of the periods determined by the laws are sentenced to imprisonment from one year to two years if they do not fulfill their duties.*

When considering the articles above, the Criminal Code must be taken into consideration as a whole and it should not be forgotten that provisions regarding deduction of the penalties can be applied by the court during the trial process according to the merits of each case. Moreover, provisions of the Code of Criminal Procedure must be taken into consideration as well.

1 https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5 .

2 https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5 .

1.3. The Law on Protection of Personal Data

The few provisions in Criminal Code explained above simply could not follow up with the complex nature of the technology during the times where millions of datas are transferred each day and a new law; the Law on the Protection of Personal Data no 6698 (hereafter LLPD) came into force.[3] As well as being the first of it's kind, protecting data by regulating the whole process from data collecting to destruction, the law is also considered as a step for harmonising legislation of Turkey with legislation of the EU by basing some provisions on Data Protection Directive of the EU. However, after the LPPD came into force the EU introduced a new legislation regarding data protection; the GDPR. As a result, the LPPD could not reach the aim of being closer to the EU legislation. However, being the first of its kind, since 2016 with the establishment of The Personal Data Protection Board (Board) and publishing of various guidelines and regulations, the law has been succesfully regulating the data protection and already shaped the process completely for each entity and natural person who process personal data. [4]

Despite not being a part of judicial, since its establishment the Board has been working as the decision maker organ for violation of protection of personal data of the cases that falls out of the scope of the Criminal Code.[i]

There is no doubt that each and every data should be kept in private and used accordingly to the law, however, some personal data must be handled more carefully than others. The LPPD divides personal data into two categories as personal data and sensitive personal data and enforces different processes for each.

According to LPPD, personal data is defined as any information that can be used to indentify a natural person. The information must belong to a natural person, any information related to a legal person or an entity is not protected under the LPPD.

a. Proceeding of Personal Data

The scope of personal data varies in a extent from very basic information such as name and surname to more complex data such as social security number. According to LPPD, personal data can not be processed without explicit consent of the natural person, all the exceptions are mentioned clearly on the 5th article of LPPD and consist of the following circumsitances:

- If clearly proposed under laws.
- If mandatory for the protection of life or to prevent the physical injury of a person, in cases where that person cannot express consent or whose consent is legally invalid due to physical disabilities.
- If necessary for and directly related to the establishment or performance of a contract, and limited with the personal data related to the parties to the contract.
- If mandatory in order for a data controller to fulfil its legal obligations.
- If the data is made manifestly public by the data subject.
- If mandatory for the establishment, exercise or protection of certain rights.
- If processing the data is mandatory for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject or any related person are not compromised.

Explicit consent is defined as consent that is related to a specified issue, declared by free will

[3] https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5 .

[4] https://gun.av.tr/tr/goruslerimiz/makaleler/the-new-personal-data-protection-law-2019-in-turkey .

and based on information[5], expressed in writing. Transfer of the personal data can be made with explicit consent of natural person whose data is being transferred. However, under some circumsitances data can be transffered without explicit consent. To transfer personal data to a foreign country, the destination country must provide sufficient protection and be marked as a safe country by the Board. According to article 9 of LPPD, a country is marked safe after consideration of certain issues by Board.

Article 9 subparagraph 4: *The Board shall determine whether there is sufficient protection in the foreign country and whether a permit will be granted pursuant to subparagraph (b) of the second paragraph;*
a) International conventions to which Turkey is a party,
b) The reciprocity of data transfer between the country requesting personal data and Turkey,
c) Regarding each concrete personal data transfer, the nature of the personal data, the purpose and duration of its processing,
d) The relevant legislation and practice of the country to which the personal data will be transferred,
e) It decides by evaluating the measures undertaken by the data controller in the country to which the personal data will be transferred, and by taking the opinion of the relevant institutions and organizations if needed.

However, a big uncertainity remains since so far no country has been marked as a safe country by the Board and neither the exact criterias are for "sufficient protection" has been announced.

In a decision dates 22/07/2020, numbered 2020/559, the Board decided that the transfer of personal data without explicit consent to a foreign country, which also is a party of the The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) of Council of Europe, was a violation and ruled a considerable amount of fine for the data controller.[6] This decision of the Board has caused arguments regarding the definition of "safe country" since the destination country has already been a party of the Convention No. 108, which Turkey is a party of and was discussed by many professionals that the decision is in contrast with the article 9 of LPPD. In addition, no specific list or any other criteria than "providing sufficient protection" had been announced by the Board. Apperantly, which country is safe to transfer personal data remains unclear.

b. Proceeding of Sensitive Personal Data

Although LPPD allows proceeding of personal data without explicit consent under certain conditions, proceeding of sensitive personal data is regulated by more strict regulations. Firstly, according to the 4th subparagraph of article 6, during proceeding of sensitive personal data, it is also obligatory to take adequate measures determined by the Board. Sensitive personal data is divided into two categories as personal data on health or sexual life and the other sensitive personal data such as religion, ethnicity, clothing etc. Proceeding processes without explicit consent also differs based on the division.

Article 6, subparagraph 3- *Personal data other than health and sexual life may be processed without seeking the explicit consent of the person concerned, in cases stipulated by the laws. Personal data related to health and sexual life can only be used for the purpose of protecting public health, performing preventive medicine, medical diagnosis, treatment and care services,*

[5] https://gun.av.tr/tr/goruslerimiz/makaleler/the-new-personal-data-protection-law-2019-in-turkey .

[6] https://www.kvkk.gov.tr/Icerik/6790/2020-559 .

planning and managing health services and financing, by persons or authorized institutions and organizations under the obligation of secrecy without seeking the explicit consent of the person concerned.

The reason why LPPD divides sensitive personal data is based on the importance and limited grounds for proceeding of data on health and sexual life. In addition, as stated in the article, personal data on health and sexual life can only be proceeded by authorised persons, who are usually health workers that are under confidentiality obligations. As explained in the article, sensitive personal data on health and sexual life can only be proceeded for purpose of the followings:

- Protection of public health.
- Protective medicine.
- Medical diagnosis.
- Treatment and care services.

As per the importance, Board rules against violation of the data on health and sexual life strictly. In the decision dates 07/05/2020, numbered 2020/355 the Board ruled for a fine of 60,000 Turkish Liras and notified the public prosecution office in regards of the offense of "illegal giving or obtanining of personal data, article 136 of the TCC".[7] The incident took place following an application to provincial health department regarding menthal health of a pharmacist, claiming the concerned pharmacist is incapable of doing the job properly and shall not be allowed to start his own pharmacy. The applicant presented a list of the medicines the concerned pharmacist uses in the form of a printed document downloaded from Medula platform.[ii] Following the investigation, it was understood the applicant received the information in Medula system with the help of his wife; who is a pharmacist.

Board ruled the violation of health and sexual data had occured. The pharmacist, who is under the obligation of keeping the data safe as the data controller had been convicted 60.000 TL fine for not providing safety of the data.[iii]

In an incident Board ruled that the transfer of personal data, even the sensitive ones, is not always ruled in the scope of LPPD. With the decision dates 30/06/2020 numbered 2020/507,[8] Board ruled that data of a deceased on health and sexual life can be transferred to their legal heir if demanded. Following death of his father, the son as the heir demanded the transfer of health data of his father, basing his demand on Regulation on Personal Health Data article 11,[9] from state authorities however his demand was declined by the data controller because it violates the LPPD.

Article 11 – *(1) The legal heirs of the deceased are individually authorized to receive the health data of a deceased person by presenting the certificate of inheritance.*
(2) The health data of a deceased person shall be kept for at least 20 years.

Under Turkish Civil Code, protection of personality of a human ends with death of the brain; even if the body is considered alive with a working heart etc. the body is not considered as a person legally and is not protected. Since the personality of the decased is not legally protected (the LPPD protects only data of real persons) and the case in question is in regards of inheritance law, The Board ruled that the demand is in the scope of Civil Code and is not in the scope of LPPD.

In the decision dates 20/05/2020, numbered 2020/407 Board fined an hospital 100.000 Turkish Liras for failing to provide

[7] https://www.kvkk.gov.tr/Icerik/6767/2020-355 .

[8] https://www.kvkk.gov.tr/Icerik/6926/2020-507 .

[9] https://www.resmigazete.gov.tr/eskiler/2019/06/20190621-3.htm .

security of sensitive personal data by transfering it to third parties without explicit consent and without a valid legal reason.[10] The incident took place when the patient who received her test results via e-mail, noticed that the e-mail was also sent to two other e-mail adresses. After demanding information regarding the incident by legal notification, as the data controller the hospital accepted the incident. Following the patients application to the Board, the hospital accepted that the results were also sent to another doctor and the assistant, who are not in charge of treatment of the person concerned. Board ruled for 100.000 TL fine for not providing sufficient protection of sensitive personal data by transfering sensitive personal data on health and sexual life to third parties.

c. Destruction of Personal Data

According to article 7 of the LPPD, once the valid reason for keeping the data expires, even if processed in accordance with the provisions of the law, personal data must be deleted, destroyed or anonymized by the data controller, ex officio or upon the request of the data subject. According to the article 11 of the LPPD, the person concerned is entitled to demand the destruction of personal data if there is no valid legal ground for keeping the data. Violation of the article 7 may meet convictions of the Board. In addition, the data controller must have a destruction policy notified to the Board before collecting and proceeding of any kind of data.

In the decision of the Board numbered 2020/93 dates 06/02/2020,[11] the Board ruled that destruction of personal data on health is not convenient since the destruction poses a serious threat to public security and public order. The person concerned demanded destruction of the data regarding his psychiatric diagnosis, stating that the records of the diagnosis cause discrimination against him specifically during employment processes.

Article 13 of Regulation on Personal Health Data regulates the cases in which the person concerned believes the diagnosis does not reflect reality.

Article 13: *The person concerned applies to the provincial health directorate to which the health service provider, for which the health data was created, is affiliated, in order to correct the inadvertently created health data about them. If the provincial health directorate finds out that the health data was created inadvertently, it will carry out on the relevant health service provider then will apply to the General Directorate with an official letter and requests for the correction of the inadvertently created health data*.[12]

As seen on the article, the destruction or change of a diagnosis can be done only in cases which the diagnosis was inadvertently created, after following a certain process. As explained above, according to the LPPD only the authorised officers can view the data on health and can keep it for specific purposes without explicit consent. In this case, in addition to absence of any legal ground for destruction of the data of the diagnosis, the diagnosis and relevant datas which are on health had been viewed by the authorised officers for relevant purposes; so the privacy was not violated and the person concerned provided the data to third parties with their own explicit consent. The Board ruled that the conditions for the processing of personal health data which are protection of public health, preventive medicine, medical diagnosis, execution of treatment and

[10] https://www.kvkk.gov.tr/Icerik/6914/2020-407.
[11] https://www.kvkk.gov.tr/Icerik/6875/2020-93.
[12] https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm.

care services, planning and management of health services and financing are still valid and keeping the data serves for these purposes. Therefore, the application of the person concerned for the destruction of the data was rejected.

2. CONCLUSION

With the LPPD coming into force, the proceeding of personal data has changed remarkably. The LPPD regulates the proceeding process from starting of collection of personal data till the destruction. The LPPD regulates proceeding of each data that is considered as personal data, however has more strict provisions for sensitive personal data and specifically for sensitive personal data on health and sexual life. Data controllers must follow the true path of proceedings of personal data carefully to avoid considerable amounts of fines. Apperantly, in the future the role of the LPPD will be more significant in our lives.

ENDNOTES:

[i] In cases which a Constitutional right is violated, the first application must be made to the first degree court according to merits of the violation, application to the Court of Constitution can not be made directly. The application process to Court of Constitution will not be explained in this article.

[ii] Medula platform is an online platform which enables the users to reach information regarding the medicines and health diagnosis of patients, with access only for relevant officers such as health or social security workers.

[iii] The process in the prosecution office for the alleged offense is not held in this article.