# Pandemic Tracking Apps and Monitoring of Personal Data Report

Faruk Çayır

alternatif bilişim

Avrupa Birliği sivil düşün

# PANDEMIC TRACKING APPS AND MONITORING OF PERSONAL DATA REPORT

November 2020

ISBN 978-605-80007-5-9

Author:
Faruk Çayır

Translation:
Hale Eryılmaz

Cover Design:
Cemgazi Yoldaş



Alternative Informatics Association
(Alternatif Bilişim Derneği)
Dikmen Caddesi No:220-B/8 Çankaya/Ankara
+90 312 230 1560
bilgi@alternatifbilisim.org
http://www.alternatifbilisim.org

This book was produced with the financial support of the European Union within the framework of European Union Sivil Düşün Programme. Its contents are the sole responsibility of Alternative Informatics Association and do not necessarily reflect the views of the European Union.

# Contents

# PREFACE

The Covid-19 pandemic, which has affected the whole world, has carried with it many questions and problem areas to the agenda. Some of these problem areas are the rising concern about the protection of personal data with the transfer of all communication activities to digital media and the increase in hate speech produced in the digital media. As the Alternative Informatics Association, we believe that monitoring, reporting and sharing these problem areas is an important effort in terms of creating awareness about and contributing to the fight against these problems that became apparent with the pandemic. With such a responsibility, we undertook the production of webinar materials to develop monitoring, reporting and digital literacy on two subjects within the scope of the "Things That Bind Us" support given to non-governmental organizations during the Covid-19 pandemic process by the European Union Sivil Düşün Programme. In this context, Faruk Çayır, the President of our Association, prepared the **Pandemic Tracking Apps and Monitoring of Personal Data Report**, and İlden Dirini and Gökçe Özsu prepared the **Report on Hate Speech in Social Media in the Covid-19 Pandemic Period** under the editorship of Assoc. Prof. Zeynep Özarslan, member of our association.

The pandemic tracing applications that were developed in almost all countries and became a part of daily life during the Covid-19 pandemic period, should be monitored and evaluated in the context of protection of personal data. Therefore, the first report evaluates the "Life Fits Home (HES)" application, specific to Turkey, on the basis of protection of personal data. Ministry of Health in Turkey implemented data surveillance based HES in order to prevent the spread of the pandemic. Technological solutions such as HES must be implemented by the public authority in a fair, transparent and accountable manner. As set out in our monitoring report, technological solutions such as HES are an outcome of political decision/will and contact tracing applications "will ensure that governments have a great oversight power; since sensitive data of individuals such as health, gender, age, language, religion, race, ethnic origin, nationality, immigration status or disability are processed, there is a serious risk of creating prejudice and discrimination in the society."

Another fact that attracts attention in the pandemic period is the increase in and intermingling of various types of hate speech in the social media platforms in Turkey. Therefore, our second report deals with hate speech on social media platforms of YouTube, Instagram, Facebook and Twitter, the types of hate speech, and the mechanisms of processing/legitimizing and naturalizing them as a discourse. The report demonstrates with examples how the increasing hate speech against particularly Chinese people, people over the age of 65 and LGBTI+ individuals is produced and circulated with user-generated content.

Finally, we prepared a webinar series by having talks with experts and academicians on the issues of societies that became data, data surveillance, surveillance capitalism, digital security, personal data, protection of personal data, and pandemic tracing applications. In particular, we aimed to answer the question of what we can do about “protection of personal data” as non-governmental organizations and citizens, with these webinars uploaded to our Association's YouTube channel.

With these works, we aim to raise awareness about the right to data, protection of personal data and hate speech in social media, among citizens and all non-governmental organizations working on right-based issues. These reports are shared free of charge in Turkish and English on the website of our Association within the scope of open access and open science policy.

We wish that the **Pandemic Tracking Apps and Monitoring of Personal Data Report** and the **Report on Hate Speech in Social Media in the Covid-19 Pandemic Period** shall reach their readers, and the awareness of freedom of expression, right to data, transparency, accountability, access to information, open source and free software that we care about as the Association shall be implemented.

**Prof. Dr. Mutlu Binark and Dr. Yeliz Dede Özdemir**
**Project Coordinators**
**Ankara 26 September 2020**

## I- PROTECTION OF PERSONAL DATA

In our country and all over the world, studies and arrangements have been made for many years regarding the protection of personal data, but the issue of protection of personal data is rapidly changing in the face of the development of communication technologies. Due to the widespread use of services of information technologies globally and increasing data traffic between countries, personal data has acquired international importance socially and economically. Many factors, such as social networks, cloud computing, big data analysis, location-based services and technological developments such as smart cards and the imperatives of globalization, deeply influence and change the methods of accessing, collecting and using personal data. Therefore, steps have been taken globally to harmonize the data protection legal infrastructures of countries with current technological developments.

Protection of personal data is an indispensable right in terms of freedom of expression, which is a basic human right. One of the first regulations in the field of protection of personal data in Turkey is the arrangement made to the 20th article of the Constitution with the Constitutional amendment made with the referendum of 12 September 2010. However, the article in question determined that the regulation would not be sufficient alone and that the field would be regulated by a special law. The Constitutional amendment in 2010 tried to clarify the issue with the following arrangement made to the 20th Article of the Constitution entitled Privacy of Private Life: *"Everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/her personal data, and to be informed whether these are used in consistency with envisaged objectives. Personal data can be processed only in cases envisaged by law or by the person's explicit consent. The principles and procedures regarding the protection of personal data shall be laid down in law."*

It should be noted that the 1981 Council of Europe Convention No. 108 constitutes an important problem in terms of Turkish Law legislation. The "Convention for the protection of individuals with regard to automatic processing of personal data,"[1] known shortly as Convention No. 108, was opened for signature in 1981 and signed by Turkey immediately. The contract entered into force in 1986. However, the Convention No. 108 only establishes general principles regarding the protection of personal data. The implementation of the Convention will be possible

[1] See, http://www.avrupakonseyi.org.tr/antlasma/aas_108.htm.

through the arrangements to be made in the domestic law of the State parties. Turkey has not made any legal regulations concerning the protection of personal data for a long time and the Law on the Protection of Personal Data No. 6698entered into force in 2016. Although the law and secondary regulations are considered to provide adequate protection on paper, exceptions regarding the processing and transfer of personal data, and regulations regarding public institutions and organizations processing personal data do not provide adequate standards for data protection.

The EU Data Protection Directive 95/46 / EC, which came into force in the EU in 1995 on the protection of personal data, provides a globally accepted framework for the protection of personal data. However, because of the technological developments we have mentioned, the need for a comprehensive reform has emerged in the EU data protection rules implemented by the European Commission, in order to modernize the principles adopted in the Data Protection Directive and to guarantee the right of citizens to privacy in the future.

After the EU member states started to transpose the EU Data Protection Directive 95/46 / EC into their domestic laws with different applications since 1995, problems began to arise in terms of unity of EU law enforcement. At the same time, the need to make the protection of personal data more compatible with the developing digital world has emerged. On the other hand, the need for a new regulation has become increasingly compulsory due to the concrete conflicts between individuals and states, and the political dilemmas of the states that make change inevitable. The violations of privacy, revealed by Edward Snowden in 2013, are at the top of these incidences though they were not directly related to the issue, but they were of great relevance regarding their impact. Apart from this, in the case known as Cambridge Analytica Scandal in the elections held in the USA, the fact that Facebook sold personal data and that the data was used for guidance and manipulation in the elections, once again revealed the importance of protecting personal data.

Snowden's statements not only caused the Court of Justice of the European Union to adopt a significant change in current legal practices, but also rigidified the general understanding in Europe regarding the protection of individual’s rights on the Internet.

The following decisions taken by the Court in this framework required a new and comprehensive reform on the protection of personal data.

- Google-Spain decision on the right to be forgotten,
- The Irish Digital Rights decision, which invalidates the 2006/24 / EC Data Retention Directive, regarding the requirement of the existence of reasonable

suspicion of crime for a possible investigation, inquiry and prosecution of the crime regarding the storage of e-mail communication data by mobile or internet phone.

- M. Schrems-Data Protection Commission Decision which invalidates the Safe Harbor Agreement due to the lack of an equivalent level of protection regarding the retention of personal data in the USA by Facebook.

In this context, the "General Data Protection Regulation -GDPR", which constitutes a radical reform in EU data protection rules, was approved by the European Parliament on 14 April 2016. The EU General Data Protection Regulation-GDPR[2] came into force on 25 May 2018.

It is also important in terms of its bindingness that the European Union makes this arrangement as Regulation. In general, when regulations come into force, they have power in all member countries. In addition, they do not require an approval law to be transposed to domestic law or a new law on the same regulations in domestic law.

However, the situation is different for the directives. The directives target the member states and impose on them the duty to make regulations in the domestic law within a certain period and within the framework specified in the directive. The method of regulation in domestic law is at the discretion of the member state. In this respect, the EU General Data Protection Regulation is a regulation that member countries are obliged to comply with without the need for regulations and approvals.

The EU General Data Protection Regulation (hereinafter referred to as GDPR) introduces new definitions, approaches and requirements for the protection of personal data. Article 3 of the Regulation makes following statement in this regard:

"2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

---

[2] See, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1797-1-1.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

Accordingly, the GDPR provisions also appear to be binding in terms of cloud service providers whose servers are located outside the EU and whose processing activities are carried out from outside the Union countries, and for those providing goods and services for people in the EU countries. In this respect, Turkey needs to bring her legal arrangements regarding protection of personal data into conformity with the GDPR.

The issue of protecting personal data, which has frequently been on the agenda during the Covid-19 pandemic, has actually been in our legal world since 1981. Although Turkey had made arrangements in this regard with various stages and occasions, the exceptions at the draft stage of the "Law on Protection of Personal Data"[3] numbered 6698, which was accepted by the Turkish Grand National Assembly on 24/03/2016 and published in the Official Gazette dated 7 April 2016 and numbered 29677, were ignored. In addition, the criticisms about the structure of the Personal Data Protection Authority, as well as the criticisms about the issues in the General Data Protection Regulation that are essential to regulate, were also ignored.

The Law on Protection of Personal Data was approved shortly before the adoption of the GDPR text, prepared within the scope of the EU Data Protection Reform, in the European Parliament. The current Law No. 6698 that entered into force on May 25, 2018 in Turkey takes as reference and is almost a translation of the 95/46/EC Data Protection Directive and European Commission's Treaty No. 108, rather than the regulations in the GDPR. Therefore, the Law No. 6698 is incomplete, inadequate and even outdated regarding many issues addressed in the GDPR

[3] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf.

## II- EU GENERAL DATA PROTECTION REGULATION AND INNOVATIONS AND REGULATIONS ON PROTECTION OF PERSONAL DATA

General Data Protection Regulation–GDPR has been adopted because of the public pressure created by many non-governmental organizations in Europe and it contains many new regulations regarding the protection of personal data and the traces of the person in digital life. Below, we will try to explain some important new aspects and regulations that did not take place in Directive 95/46/EC and the regulation to Law No. 6698:

- ***Definition of Personal Data***

GDPR tried to bring a more descriptive and comprehensive definition to personal data compared to Directive 95/46/EC and Law No. 6698. GDPR defines personal data as *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."* As can be seen, all kinds of data that are appropriate for new technologies such as location data, online identifier, and which will enable to reveal the current data owner, have been accepted as personal data.

- ***Profiling***

It is noteworthy that GDPR introduces profiling as a new definition that was not found in Directive 95/46/EC and Law No. 6698.

GDPR defines profiling *as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."*

In case personal data are processed depending on automatic decision making mechanisms, data subjects have the right to request meaningful information on the logic carried out, as well as information regarding the importance and anticipated results of the processing activity for the data subject. Data subjects have the right

not to be subject to a decision based solely on automated processing, including profiling, which has legal consequences for them or similarly significantly affects them. Data subjects have the right to object to the processing of personal data related to profiling at any time and to the processing of personal data related to them for direct marketing, and to complain to the competent authority (Personal Data Protection Board) if their objection is not accepted.

- ***Pseudonymisation***

Another new definition introduced by the GDPR that is not found in Directive 95/46 and Law No. 6698 is pseudonymisation. The GDPR defines pseudonymisation as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

The data controller must implement appropriate technical and organizational measures, such as the use of pseudonyms, designed with the aim of effectively implementing data protection principles such as minimizing data and integrating the necessary assurances to fulfill the requirements of this Regulation, and protect the rights of data subjects, both during the determination of the processing method and during the processing activity.

The controller and processor are required to provide appropriate safeguards, including the use of pseudonyms and encryption on personal data, to ensure an appropriate level of security in terms of risk, taking into account the risks of various possibilities and seriousness to the rights and freedoms of natural persons.

Pseudonymous data is not anonymization of personal data but a method of de-identification of data. If the data processed by the controller does not allow the controller to directly identify a person or creates pseudonymised data, the controller may not receive or process the additional information in order to identify the data subject only to comply with this regulation. Pseudonymous data is information that no longer allows the identification of an individual without additional information and is kept separate from it. In this sense, it also requires protection for pseudonymous data.

This type of personal data, called pseudonym data, is a good example of data protection in terms of risk-based approach and liability. Because the data controller and the data processor will have to take all reasonable precautions to ensure that

the data remains pseudonymous data and to prevent the data from becoming fully correlative.

- ***Right to erasure ('right to be forgotten')***

The right to be forgotten is regulated under Article 17 of the GDPR under the heading of the data subject's right to request erasure of personal data. With this article, it is seen that the scope of the right to erasure of personal data granted to the data owner in Law No. 6698 and in Article 12 (b) of Directive 95/46 is extended. According to this article,

> "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
>
> - the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
> - the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
> - the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing.
> - the personal data have been unlawfully processed;
> - the personal data have been collected in relation to the offer of information society services to a child

Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data."

As can be understood from this article, data subjects have the right to request their data to be erased or not to be further processed in cases where their data is no longer required to be kept in relation to the purpose of collection, the data owner does not have their consent or the data subject does not want their data to be processed, or the personal data is processed contrary to the GDPR. It appears that the

data controller is also responsible for erasure of shortcuts, copies or duplicated versions of personal data if they have shared or made available personal data with other data controllers.

With this regulation, an important right has been granted to data owners who have lost audit and control over their data, in de facto and legal terms, especially through algorithms and other automatic data processing methods.

The right to be forgotten accepted under the GDPR is not included in Law No. 6698. However, regarding the right to be forgotten; In the decision of the 4th Civil Chamber of the Supreme Court of Appeals dated 03.07.2013 and based on 2013/6256, "the personal rights of the victim of sexual harassment were violated because the name of the victim of sexual harassment was published in a book without coding" and the compensation was ruled for this reason. In its decision dated 03.03.2016 / No. 5653, which was about the appeal of a person who asked the news made about him/herself on the Internet be removed, the Constitutional Court found the applicant right.[4] Therefore, the right to be forgotten found itself an implementation are by the decisions of the judiciary. The fact that right to be forgotten, which has been accepted by the judicial decision, was not included in the legal regulations caused criticism during the construction process of Law No. 6698. For this reason, Turkey should prepare an emergency legislation on the right to be forgotten, which is given a great importance by EU member states.

[4] According to the Constitutional Court 's decision dated 03/03/2016 and numbered B.2013 / 5653: "The right to be forgotten is not clearly regulated in our Constitution. On the other hand, in the 5th article of the Constitution under the heading of "the main purposes and duties of the state", the expression "trying to prepare the necessary conditions for the development of the material and spiritual existence of human beings" imposes a positive obligation on the state. In the context of this obligation, considering the right to protect the honor and reputation of the person in the context of the moral integrity of the person regulated in Article 17 of the Constitution and the right to request the protection of personal data guaranteed in the third paragraph of Article 20 of the Constitution, it is clear that the state has a responsibility to prevent others from learning about the past experiences of the individual and to allow ”to open a new page”. In particular, the right to request the deletion of personal data within the scope of the right to protect personal data includes enabling the past negativities of individuals to be forgotten. Therefore, the right to be forgotten, which is not explicitly regulated in the Constitution, appears as a natural consequence of Articles 5, 17 and 20 of the Constitution in order to prevent access to news that is easy to access via the Internet and stored in digital memory. On the other hand, the non-acceptance of the right to be forgotten makes the intervention permanent that prevents the individual from living a dignified life and maintain spiritual independence because it leads to creation of prejudices about the individual by others due to the fact that personal data can be easily accessed via the Internet and can be stored for a long time. See https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/5653.”

- ***Right to data portability***

Another new regulation introduced by the GDPR that is not found in Law No. 6698 and Directive 95/46 is data portability. Article 20 of the GDPR reads as: “The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on consent… or on a contract; and the processing is carried out by automated means.”

When using the right to data portability, the data subject has the right to ensure the transmission of personal data directly from one controller to another, if technically feasible. The exercise of the right to data portability does not eliminate the right to request erasure of data (right to be forgotten). This right does not apply to the processing activities required for the fulfillment of a duty in the public interest or for the enforcement of a formal mandate given to the controller.

- ***Data Controller and Data Processor Distinction, All Data Processors Being Responsible for Data Processing***

In Directive No. 95/46, the only person who is obliged to comply with the rules regarding the processing of "any data related to an identified or identifiable natural person" and who is responsible for unlawful work and transactions is the "data controller", in other words, it was arranged as the person who had the data ownership. With the GDPR, a triple data ownership and responsibility regulation has been introduced as controller, processor and receiver.

The controller is a natural or legal person, public authority, institution or any other body that alone or jointly with others determines the purposes and methods of processing personal data.

Processor is a natural or legal person, public agency, institution or any other body that processes personal data on behalf of the controller.

Recipient is a natural or legal person, public institution, or any other body to whom personal data are disclosed, whether it is a third party or not.

With the regulation introduced in the GDPR regarding data ownership, any company or individual, although they are not data controllers, that processes this data (including third parties that provide sub-services such as cloud service providers) will be held responsible for the processing of the data in accordance with the law.

Whether this regulation is automatic or not, those who implement any transaction or sequence of transactions such as collecting, saving, editing, structuring, storing, adapting or modifying, obtaining, consulting, using, disclosing, disseminating or making available, harmonizing or combining, restricting, deleting or destroying personal data or personal data sets, i.e. all perpetrators of any processing activity (controller, processor, recipient) are liable for any data breach and illegality arising from the processing in question.

The repercussions of the implementation of this provision will be quite wide. Legal responsibility arises for both data controllers and third parties who process data at the request of the data controller. In this context, the GDPR provisions will be binding for cloud service providers whose servers are located outside of the EU and that maintain their processing activities from outside the Union countries and for organizations that provide goods and services to EU member countries. In this case, the high fines imposed by the GDPR for this organization or persons engaged in erroneous and unlawful processing are also binding for these processors.

- ***Consent of the Data Subject***

The "explicit" consent of the data owner was emphasized in the Law No. 6698 and Directive No. 95/46 regarding the consent of the data subject, which makes data processing legal. In GDPR, a strengthened concept of consent in favor of the data subject is remarkable. In the “definitions” section of the GDPR, the consent of the data subject is defined as any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

In addition, according to Article 7 of the regulation, if the data subject’s consent is given in the context of a written declaration that also concerns other matters, the request for consent shall be presented in a manner, which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration, which constitutes an infringement of this Regulation, shall not be binding. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia,* the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

As can be seen, the consent for the processing of personal data must be given freely, in a specific, enlightened / purposeful, conscious and explicit manner. The

consent in question must be obtained in terms of all processing activities carried out by the data processor for the same purpose or purposes. Likewise, in cases where consent is requested by electronic means, this request should be simple, clear and in a nature that does not prevent the use of the service the consent is required for.

On the other hand, if users remain silent about the privacy settings of online social networks or web browsers, or have not made any objections until then, the default settings will mean that there is no valid consent.

- ***The withdrawal of explicit consent***

Likewise, according to the arrangement made by Article 7 of the GDPR, the data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. According to the regulation, the data subject has the right to withdraw his freely given consent at any time. While this wide range of rights and powers brought by the GDPR provides data owners with a very large area to determine the fate of their data, it imposes very detailed responsibilities on data processors.

- ***Conditions applicable to child's consent in relation to information society services***

According to the new regulation introduced by Article 8 of the GDPR, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child. The controller shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology.

As can be understood from this regulation, a possible violation of rights in the future has been considered regarding the use of communication technologies and social media by today's children. The age limit of 16 has been observed in the processing of personal data of children, and Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.

- ***Rights of the Data Subject***

According to Article 13 of the GDPR:

1. "Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
(b) the contact details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

As can be seen, the GDPR grants broader rights and powers to the data subject compared to the Law No. 6698 and Directive No. 95/46 in order to ensure a fair and transparent processing at the time when personal data are obtained.

- ***The Data controller's obligation to provide transparent information, communication and modalities for the exercise of the rights of the data subject***

In Article 12 of the GDPR, the obligation to inform about the user rights is left to the data controller. According to the article, "The controller shall take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The controller shall facilitate the exercise of data subject rights."

Likewise, Article 24 of the GDPR reads as: "Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood

and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."

When these regulations are considered together, data controllers are obliged to inform their users and make the necessary reminders about their legal rights within the scope of the GDPR, and are obliged to document that they fulfill their obligations.

According to Article 25 of the Regulation, "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, **the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures**, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

Again, when these provisions are evaluated together, if the personal data of the users will be stored in the controller's systems, the person must give absolute consent under any circumstances. In this system, everyone has the right to leave the system free of charge, easily and quickly. If this rule is violated, data controllers will have to pay heavy damages.

At the same time, according to Article 25, the data controller should determine its internal functioning policies and take the necessary measures to meet the principles of data protection from the outset of data processing and privacy and data protection from design. The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements for protection of the rights of data subjects. The data controller must ensure that personal data of the data subject are not made accessible to an indefinite number of persons without any initiative of the data subject. This obligation of the controller is valid at the time the data is collected and during its processing, as long as the personal data is stored and the data is accessible.

- ***Data protection officer***

According to Article 37 of the GDPR, "The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10."

As can be understood from this article and as cited in Article 9, "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. However, in case of processing due to exceptions, in any case, the data processor must have a data protection officer with sufficient expertise in the field and this data protection officer is responsible for the processing."

According to this regulation in the GDPR, it is possible for the data protection officer to be employed by an employment contract, as well as the data protection officer to work on behalf of more than one company or public institution.

- ***Mandatory Data Protection Impact Assessment in Terms of Risky Data Processing Activities***

According to Article 35 of the GDPR, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons. The third paragraph of the Article states that a data protection impact as-

sessment (DPIA) shall be required in the case of a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling; processing special categories of data or of personal data relating to criminal convictions and offences or a systematic monitoring of a publicly accessible area on a large scale.

As can be understood, it is stated that the results of the said DPIA will be taken into account in determining the measures to be taken for the realization of personal data processing activities in accordance with the provisions of the GDPR. It is emphasized that DPIA is necessary especially in large-scale processing activities.

In addition, if it appears as a result of a VKED that processing activities comprise a high risk not eased with appropriate measures in terms of available technology and implementation costs, Personal Data Protection Authority (KVKK), which is the supervisory authority for Turkey, should be consulted before starting data processing activity. The KVKK, the supervisory authority, creates a list of types of processing activities that are or are not subject to impact assessment requirement concerning data protection and will disclose this list to the public.

Since the general provision regarding the notification of data processing activities to the data protection authorities, as stated in the Directive No. 95/46, does not provide a rooted solution for the protection of personal data, it is thought that it would be much more appropriate to make the VKED instead of this general notification obligation defined by the new regulation without discrimination. In VCED, the data controller will be able to consider the purpose and scope of the processing and the sources of the risk before assessing the high-risk probability and severity.

## III- PROTECTION OF PERSONAL HEALTH DATA

Health data are personal data of special nature within the scope of Law No. 6698.[5] According to Article 6 of the Law:

> (1) Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the 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 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 of the data subject, in the cases provided for by laws. Personal data concerning health and sexual life may only be processed, without seeking explicit consent of the data subject, by the persons subject to secrecy obligation or competent 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

Sub-clause (ç) of Article 28 of the Law states that personal data are processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorized and assigned by law to maintain national defense, national security, public security, public order or economic security. As it can be understood from this statement, for reasons such as epidemic diseases, preventive health practices, natural disasters, emergency practices, mass demonstrations, etc. personal health data can be personally recorded and processed not only by a public institution, but also by more than one public institution and organization, as well as data transfer between institutions.

[5] See, https://www.kvkk.gov.tr/Icerik/4110/2018-10.

With the decision of the Personal Data Protection Board, dated 31.01.2018 and numbered 2018/10, regarding the processing of special categories of personal data, "Conditions for Processing of Special Categories of Personal Data" were determined as follows:

> "1- Determination of a systematic, clearly defined, manageable and sustainable separate policy and procedure for special categories of personal data
>
> 2- For employees involved in the processing of special categories of personal data the following are required:
>
> a) Regular training on the law and related regulations, and security of special categories of personal data,
>
> b) Making confidentiality agreements,
>
> c) Clear definition of the scope and duration of the authority of those who have the authority to access data,
>
> ç) Periodic authorization checks,
>
> d) Immediate removal of the authority of employees who have a change of position or leave their jobs. In this context, the return of the inventory allocated to the employee by the data controller.
>
> 3- If the media where special categories of personal data is processed, stored and/or accessed is electronic media, the following are required:
>
> a) Storage of data using cryptographic methods,
>
> b) Keeping cryptographic keys in secure and different media,
>
> c) Secure logging of process records of all transactions performed on data,
>
> ç) Continuous monitoring of the security updates of the media where the data is kept, performing/having the necessary security tests on a regular basis, recording of test results,
>
> d) If the data is accessed through a software, making user authorization of this software, making/ having made the regular security tests of these software, and recording test results,
>
> e) Providing at least two-step authentication system if remote access to data is required

4- If the media where special categories of personal data are processed, stored and/or accessed is a physical environment, the following are required:

a) Ensuring that adequate security measures (against electrical leakage, fire, flood, theft, etc.) are taken depending on the nature of the environment where special categories of personal data are kept,

b) Ensuring the physical security of these environments and preventing unauthorized entry and exit.

5- If special categories of personal data will be transferred

a) If data need to be transferred via e-mail, transferring them in encrypted form using a corporate e-mail address or a Registered Electronic Mail (REP) account,

b) Encrypting it with cryptographic methods if data needs to be transferred via media such as Portable Memory, CD, DVD and keeping the cryptographic key in different media,

c) If transfer is made between servers in different physical environments, transferring data between servers by setting up VPN or by sFTP method is required.

ç) If the data is to be transferred in paper form, necessary precautions should be taken against the risks such as theft, loss or being seen by unauthorized persons and the document should be sent in the "confidential documents" format.

6- In addition to the above-mentioned measures, technical and administrative measures to ensure the appropriate level of security specified in the Personal Data Security Guide published on the website of the Personal Data Protection Authority should also be taken into consideration."

Especially in the processing of health data, the general (basic) principles in the processing of personal data specified in Article 4 of Law No. 6698 should be regarded: "The processing must be in accordance with the law and honesty rules, being accurate and up-to-date when necessary, being processed for specific, clear and legitimate purposes, being linked, limited and proportionate to the purpose for which they are processed, and kept for the period stipulated in the relevant legislation or required for the purpose for which they are processed".

In this respect, according to Article 9 of the GDPR titled “processing of special categories of personal data”, the processing of personal data in special categories cited below is possible with the condition that "appropriate and specific measures are taken to ensure the fundamental rights and interests of the data subject, which are proportionate to the pursued purpose, respecting the essence of the data protection right":

> g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
>
> h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
>
> i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

In this context, since the current situation threatens general public health, public security and public order, there is no legal obstacle to the processing of personal data by the Ministry of Health and public institutions and organizations covered by the above article. However, this does not eliminate the fact that during the collection of health data through various applications and practices by public institutions and organizations such as the Ministry of Health, they must take the specified technical and administrative measures, which are proportionate to the purpose pursued, respect the essence of the right to data protection, and that appropriate and specific measures must be taken to secure the fundamental rights and interests of the data subject.

## IV- DECISIONS OF THE PERSONAL DATA PROTECTION AUTHORITY DURING THE PANDEMIC PROCESS

The following statements were made by the Personal Data Protection Authority on various dates regarding the protection of personal data during the pandemic process:

- The statement dated 27/03/2020 reads as: “Even in these exceptional times, data controllers and data processors are required to ensure the security of the personal data of the persons concerned. For this reason, it is important that personal data are processed in accordance with the law and that any measures taken in this regard comply with the general principles of the law, and within this framework, irreversible damages will not occur in terms of the fundamental rights and freedoms of individuals. In this respect, personal data processing activities carried out especially within the scope of the measures taken against the COVID-19 virus should be necessary, relevant, limited and measured."[6]
- According to the statement dated 07/04/2020: “In the distance education platforms, it is seen that personal data such as names and surnames of students and some special personal data that can be evaluated within the scope of biometric data such as voice and image are processed. In Article 5 of the Law on the Protection of Personal Data No. 6698, the conditions for the processing of personal data, and in Article 6, the processing conditions of personal data of special nature including biometric data are specified. At this point, personal data should be processed in accordance with the conditions specified in Article 5 and / or Article 6 of the Law."[7]
- According to the statement dated 09/04/2020, "Considering that serious damages may occur for the relevant persons in the course of processing the location data of persons by associating with their health status, in case the said data is seized by third parties, the relevant institutions and organizations are required to they take any technical and

[6] https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler.-

[7] https://www.kvkk.gov.tr/Icerik/6723/Uzaktan-Egitim-Platformlari-Hakkinda-Kamuoyu-Duyurusu.

> administrative measures, and it should not be forgotten that the personal data in question shall be deleted or destroyed if the reasons requiring the processing of this data disappear."[8]

As can be seen, no information or explanation has been shared with the public about whether the contact tracing application has been subjected to necessary and sufficient controls, whether the authorized institution such as the Personal Data Protection Board has carried out audits concerning the protection of health data and other personal data, which are sensitive data.

[8] https://www.kvkk.gov.tr/Icerik/6726/COVID-19-ILE-MUCADELEDE-KONUM-VERISININ-ISLENMESI-VE-KISILERIN-HAREKETLILIKLERININ-IZLENMESI-HAKKINDA-BILINMESI-GEREKENLER-2-?utm_campaign=DonanimHaber&utm_medium=referral&utm_source=DonanimHaber.

## V- CONTACT TRACING APPLICATIONS IN COVID-19 PERIOD

In the first month of 2020, with the rapid spread of the COVID-19 virus first in China and then all over the world, and with the epidemic turning into a pandemic, most governments around the world have implemented a series of digital monitoring, surveillance and censorship measures to slow the spread of the virus and protect public health. While some of these were made in an unprecedented manner, through urgent administrative decisions without necessary and adequate scrutiny, some were put into practice by legislative bodies.

It seems that digital monitoring and surveillance applications will continue to threaten the digital rights of citizens for months or even years to come. Excessive and disproportionate technological practices, which are stated to help control the spread of COVID-19, will gradually increase the authority of governments and technology companies to access personal data. Personal data will become a natural part of security policies applied in the social field.

During the course of COVID-19, there is growing global interest in using location data held by major technology companies to trace individuals affected by the virus, better understand the effectiveness of physical distance, or send alerts to people who may be affected by those who have been contacted. It has gained great importance to measure the proximity of individuals with the people diagnosed with the disease and to known cases of the disease. This is why governments around the world have begun to consider whether and how to use mobile location data to help find the spread of the virus.

There has been a sharp increase in the number of people-tracing applications available around the world since January.[9] These apps are claimed to be designed to help prevent the spread of the virus by using location data to trace individuals and other individuals they come into contact with. Although the intentions of the developers of these applications are good, the applications raise significant concerns about --both efficiency and privacy. As many studies have shown, even some anonymized datasets are at risk of being redefined.[10] In addition, the absence of clear privacy policies and the use of centralized data storage will increase the likelihood of data being vulnerable to misuse.

---

[9] See, Çayır, F. (2020). Contact Tracking Practices and Protection of Personal Data in the COVID-19 Process. Ankara: Alternative Informatics Association https://ekitap.alternatifbilisim.org/covid-19-temas-takip-uygulamalari/.

[10] https://cpg.doc.ic.ac.uk/blog/fighting-covid-19/.

## VI- ABOUT LOCATION DATA[11]

Mobile operators and operating systems as part of the core functions of a device can capture location data, by mobile applications that are features for users, and by Internet of Things (IoT) devices, such as smart items or toys, that allow them to be tracked and emit identifying information, even if they are not connected to a network. The location data of individuals can be accessed through various means by the governments, both legally and illegally, by institutions and organizations authorized legally.[12] However, the pandemic process may turn into the authority of institutions and organizations to store and use location data indefinitely by using this emergency and extraordinary situation as an excuse and by taking an opportunity, without encountering any obstacle and without any explanation.

Location data or mobility data includes information about how devices and people move through spaces over time. In the most basic sense, the connectivity feature of a device or the ability to send and receive wireless content on the devices contains information about the location of these devices. For example, wireless service providers know where the devices are located because they provide the devices over local base stations and networks. On a more general level, an IP address (an identifier freely and explicitly shared by devices for sending and receiving Internet traffic) is usually sufficient to know a person's city and location.

Most of the time when it comes to location data, we think of GPS (Global Positioning System), but it is just one of many ways to extract the locations of devices that are actually used not only by GPS but also by operating systems, phone operators, applications and other networked devices.

GPS is a space-based satellite navigation system that provides location and time information in all weather conditions with four or more satellites in an unobstructed line of sight on the earth.[13] Smartphones and other devices can detect location via GPS regardless of any phone or internet reception.

Base stations provide network access to users. Each station has a unique number. Cell phones connect to one of these stations close to them. This also means that mobile operators can know our location approximately. HistoricalTrafficSearch,

---

[11] This section has been shortened and compiled by citing information on the website https://fpf.org/2020/03/25/a-closer-look-at-location-data-privacy-and-pandemics/.

[12] According to Article 51 of the Electronic Communications Law in Turkey, traffic and location data can be processed by telephone operators.

[13] https://tr.wikipedia.org/wiki/GPS.

also known as HTS records, shows the calls made by people on their phones. It includes information such as call time, call duration, call location and receiving base stations.

If connected to Wi-Fi networks, mobile devices can identify their location by scanning nearby Wi-Fi networks. Nearby networks or "hotspots" may include, for example, neighbors' Wi-Fi or Wi-Fi of cafes and shops. These networks have large databases of unique identifiers (MAC addresses and SSID) of wireless routers and their known locations.

In the use of Bluetooth, many applications are designed to detect their proximity to "hardware", small radio transmitters that broadcast unidirectional Bluetooth signals. An app that the user gives permission to access Bluetooth can extract the location of the device or send proximity-based alerts or other content.

Each method of obtaining location data requires a different level of precision and can be used for different purposes. Many governments and government agencies are interested in accessing "anonymous" or "anonymous and aggregated" location data to observe population-level trends and movements. While it is possible to anonymize data in some cases, it is very difficult to "anonymize" truly each exact location data and dataset. Even if unique identifiers are used instead of names, most people's behavior can be easily traced, for example, from the location of their home (whether the device is turned on, what time it is turned on, etc.). Although unique identification marks are used in terms of location data, the identity of the person or group can be easily revealed when location data and a few other pieces of information convene.[14]

According to a study on this subject, a simply anonymized dataset does not include name, home address, phone number, or other distinct identifiers. However, if the individual's patterns are unique enough, external information can be used to link data back to an individual.[15] For instance, an ill-minded person who can access to a medical database that is supposed to be converted to anonym with the unique identifier can successfully transform the person he wants to be identifiable by combining location data and a medical database with a public voter record list to find a different person's health record.

These challenges of anonymizing data are very difficult to overcome, but policymakers should be very careful not to over compromise both public power and

[14] https://www.nature.com/articles/srep01376.

[15] https://dl.acm.org/doi/abs/10.1145/2030613.2030630.

platform capitalism on the issue, and treat location data sets as private and sensitive data.[16] By predicting who can access location data and for what purposes, and ensuring that data recording is limited; administrative, technical and legal audits on location data need to be increased. In this regard, it should be emphasized that non-governmental organizations should also have an effective say in policymaking. The public authority does not open up space for relevant civil society organizations to participate in public policy-making concerning protection of personal data, marking and use of location data in Turkey.

[16] https://www.nature.com/articles/sdata2018286.

## VII- STATEMENTS OF INTERNATIONAL ORGANIZATIONS ON THE PROTECTION OF PERSONAL DATA IN CONTACT TRACING PRACTICES

UN Special Rapporteurs made a statement that states shall not abuse emergency measures to suppress human rights: “While we acknowledge the seriousness of the current health crisis and recognize that the exercise of emergency powers is permitted by international law in response to significant threats, we urgently remind States that emergency responses to the coronavirus must be proportionate, necessary and non-discriminatory.”[17]

UN / DESA (Department of Economic and Social Affairs) has called on governments to be transparent and share information about the health crisis. UN / DESA released a statement aiming at involving various stakeholders in the management of the pandemic; and accelerating the implementation of stakeholder partnerships and innovative digital technologies through appropriate privacy measures for public-private partnerships.[18]

The European Commission's Recommendation on Contact Tracing Applications suggested a coordinated approach for the use of contact tracing applications. The Recommendation fostered a common approach for modelling and predicting the evolution of the virus through anonymized and aggregated mobile location data. The recommendations included following principles: ensuring respect for fundamental rights and prevention of stigmatization respect to fundamental principles and not stigmatizing individuals; preference for the least intrusive yet effective measures; presenting technical requirements concerning appropriate technologies; effective cybersecurity requirements; the expiration of measures taken and the deletion of personal data obtained through these measures when the pandemic is declared to be under control; preference for anonymous analysis and warning systems based on proximity data; and transparency requirements on the privacy settings.[19]

By publishing the eHealth Network text on the use of health data, the European Commission has recommended paying attention to the following aspects of mobile

---

[17] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E.

[18] https://www.un.org/development/desa/dpad/publication/un-desa-policy-brief-61-covid-19-embracing-digital-government-during-the-pandemic-and-beyond/.

[19] https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.

applications that support contact tracing in the EU's fight against COVID-19: assessment of the role of contact tracing and warning; inventory of existing initiatives, and detailing the basic requirements for contact tracing at national level; voluntary use as approved by the national health authority; personal data must be securely encrypted and removed when not needed.[20]

European Commission's Guidance on Apps Supporting the Fight against COVID-19 Pandemic in Relation to Data Protection explains the features and requirements that applications must fulfill in order to comply with EU privacy and data protection legislation, especially the GDPR[21] and the ePrivacy Directive.[22]

European Union European Data Protection Board (EDPB) released Draft Guidance on Apps Supporting the Fight Against the COVID-19 Pandemic inviting the European Union states to consult the data protection authorities and urged member states to encourage certain measures regarding person tracing applications which include the following: developing applications in an accountable manner; basing on privacy as a design and default feature; having open source code; not using the system even in emergencies after the c crisis is over and any data is deleted or anonymized; being voluntary, safe and interoperable.

It was highlighted that states should enact national laws that provide a legal basis for such applications, that location tracing of individual users is not required, and that health authorities and scientists must develop a rigorous mandatory test to identify the basic functional requirements of these applications. It was underlined that decentralized applications should be used more, parallel with minimum data recording the post-test contact of individuals should be limited by health authorities in non-fully automatic ways, data should not be reused and should be deleted in a timely manner, and the redefining of contact persons of those who use the application should be prevented with the measures taken.[23]

The European Data Protection Board's (EDPB) Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak is a comprehensive booklet

---

[20] https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[21] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

[22] https://ec.europa.eu/info/sites/info/files/5_en_act_part1_v3.pdf.

[23] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf.

on the use of location data, employment, basic principles and the legality of processing.[24]

In Bulletin 4 of 'Coronavırus Pandemic In The EU – Fundamental Rights Implications' the European Agency for Fundamental Rights provides information on how to ensure privacy and data protection rights during the pandemic by data protection authorities of employers and media institutions. Especially data processing is outlined.[25]

European Commission President Ursula von der Leyen and European Council President Charles Michel signed a joint European Roadmap on April 15 to lift COVID-19 containment measures.[26] According to the joint declaration, the objective is to create a framework for person tracing and warning application with the use of mobile applications that respect data privacy. As they can help disrupt chains of infection and reduce the risk of further transmission, contact tracing applications are an important element in member states' strategies as long as they complement other measures, including increased testing capacity. It is recommended that the mobile applications be voluntary and included in system design of national health authorities. The recommended safeguards are a mix of a range of technical safeguards, such as anonymization and collection of data, tracing of users, and governance protections. When the COVID-19 crisis is over, it is necessary to delete the data saved with the application, which is transparent and has a certain expiration time, and the applications must be disabled. According to the document, trust in these apps and their respect for privacy and data protection are crucial to their success and effectiveness.

The statement made by EDRi (European Digital Rights), of which our association is a member, read as:

*"States should respect human rights when using digital surveillance technologies to combat the pandemic. An increase in undisclosed digital surveillance power and gaining access to cell phone location data could violate privacy, freedom of expression and freedom of association rights and reduce trust in public authorities, as well as undermine the*

---

[24] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

[25] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-1_en.pdf.

[26] https://ec.europa.eu/info/sites/info/files/communication - a european roadmap to lifting coronavirus containment measures 0.pdf.

*effectiveness of any public health response. These measures also carry the risk of discrimination and can disproportionately harm already marginalized communities."*[27]

Access Now has prepared a series of recommendations concerning do's and don'ts in the use of COVID-19 person tracing apps for privacy and public health.[28] The statement made by CCC (Chaos Computer Club) listed minimum 10 requirements for person tracing applications. According to the statement: "In principle, the concept of a 'Corona Application' involves a great risk because of the contact and health data that can be collected. At the same time, adhering to the principles of 'privacy by design' developed by the crypto and privacy communities in recent years, it is possible to reveal the potential of contact tracing applications with the help of these technologies without creating a privacy disaster. For this reason alone, all concepts that violate or even endanger privacy must be strictly rejected."[29] An information list has been prepared by Privacy International regarding the COVID-19 applications implemented by different countries.[30] According to the statement made by Privacy International: "The starting point for such applications is only to help health. Applications are a small part of protecting public health in combating the pandemic. Any measure should prioritize people and minimize data. People need to be confident that their data and devices are safe and that data should be destroyed at the end of this global pandemic."[31]

Free Software Foundation Europe (FSFE) made the following statement: "Free Software offers enough transparency to validate complete data protection and compliant use; thus trust can be established. Only Free Software can enable global code development in a legally safe cooperative environment. Any proprietary solution will inevitably lead to countless isolated solutions and thereby waste energy and time. Besides global cooperation, Free Software licenses allow sharing of code in any jurisdiction."[32] According to the statement made by the Electronic Frontier Foundation (EFF), "The EFF has long been struggling against the digital surveillance of our location data, health data, and personal relationships by governments and

---

[27] https://alternatifbilisim.org/stklardan-covid-19-ile-mucadele-dijital-hak-ve-ozgurluklere-saygi-cagrisi/.

[28] https://www.accessnow.org/privacy-and-public-health-the-dos-and-donts-for-covid-19-contact-tracing-apps/.

[29] https://www.ccc.de/en/updates/2020/contact-tracing-requirements.

[30] https://www.privacyinternational.org/examples/apps-and-covid-19.

[31] https://privacyinternational.org/long-read/3675/theres-app-coronavirus-apps.

[32] https://fsfe.org/news/2020/news-20200402-02.en.html.

companies, and against big data systems turning our lives into open books. This type of data processing often violates our privacy, prevents our free speech and association, and puts different burdens on minorities. Some use of big data can be warranted as public health officials work to contain COVID-19. However, it should be medically necessary as determined by public health professionals; the processing of personal data should be commensurate with actual new needs. People should not be scrutinized due to their nationality or other demographic factors, and any new government authority must end when the disease is found."[33]

[33] https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis.

## VIII- THE "LIFE FITS HOME" CONTACT TRACING APPLICATION FOR THE PANDEMIC IN TURKEY

The Ministry of Health has implemented three different applications due to the COVID-19 pandemic. Among these applications, the Corona Virus Control Application (19 March 2020) and Pandemic Isolation Tracing Project (09 April 2020) applications were combined under the name *Life Fits Home* (18 April 2020) application.[34] The *Life Fits Home* (HES) Code has been added to the *Life Fits Home* application to be used in the intercity transportation services that have been operating since June 4, 2020.

*Life Fits Home* application is an application implemented by the Ministry of Health in cooperation with the Information Technologies and Communication Authority (BTK) and GSM operators (Turkcell, Turk Telekom, Vodafone). The application monitors whether mobile phone subscribers change their location or not basing on the location data of mobile phone subscribers.

With the application, the Ministry of Health exchanges data with Mernis (Central Population System) information and E-Pulse systems.


The application involves the following:

- COVID-19 test positive and diagnosed people,
- People who have close contact with those diagnosed,
- It covers people who are under curfew according to age groups (over 65, under 20).

[34] "Hayat Eve Sığar" is the name of the application in Turkish.

The application involves the following points:

- Warning people who are required to be in isolation at home via text message service when they leave their homes
- Contact these people instantly and asking them to return to where they need to be under isolation.
- Informing the relevant police units about the situation of those who do not comply with the warning and continue with the violation, and implement the necessary administrative measures and sanctions
- Inquiry by road control police teams the information of people they control to find out whether or not the person violates isolation requirement.

The content of the application includes the following:

- Questionnaire; How do you feel today?
- Easy access to basic needs points on the map such as hospitals, pharmacies, market chains, metro and stops,
- Density; warning given when approaching risky areas where the epidemic is intense and the areas that should not be approached instantly on the map,
- My family; By adding relatives to the family section, location information and risk situations according to their regions can be viewed and followed in case the person gives consent.
- Information section.

***HES Code Application***

The HES code has been mandatory for all citizens during the Covid-19 pandemic for domestic flights, train and bus travels. The QR code, called the HES code, added to the HES application can be received via the Life Fits Home application, e-government app or SMS.

To get the HES code through the application: Enter the "HES Code Process" section on the Life Fits Home application. Click on the "Generate HES Code" button. Code usage period is selected and code is generated.

To get the HES Code via e-devlet (e-state): Enter with the e-government password and use the HES code section; you can create, delete, query and view the details.

To get the HES code via SMS: Type HES and leave a space between T.C. Identity Number, The last 4 digits of the ID Serial Number and the Sharing time (in number of days) are written and sent to 2023 as an SMS.

The generated HES codes can be shared with the institutions or individuals directly or via the mobile application. Institutions or individuals can question whether you carry any risk regarding Covid-19 by querying the HES codes you shared. Likewise, users can query shared HES codes through the application and see the risk status of people.


After the HES code is received, the HES code must be shared with the travel company. The company or institution questions the health status of the person with the HES code. Through the HES codes, it will be possible to question whether the passengers carry the risk of Covid-19 and the travel of risky people can be prevented.

The HES code is valid for a certain period. Travel companies require the HES code to be valid for at least 7 days from the date of travel; otherwise reservations are not confirmed.

According to the Application's Clarification Text[35],

*Identity of the Data Controller;* In terms of your personal data processed in this application, the data controller is the Ministry of Health.

*Purposes of Processing Personal Data;* in this application, your personal data below are processed for the following purposes, limited to the duration of combating the pandemic.

*Identity data:* Your Identity Number, father's name and date of birth are processed in order to verify your identity. You can use the application with some restrictions without entering this data. If you do not want to enter your identification number, you must enter your age in order to calculate your COVID-19 risk.

*Communication data*: Your GSM number is processed in order to enter the code to be sent via SMS when you first install the application, and to verify your phone number. Only one registration can be made for the application with each GSM number. It is not possible for more than one person to use the application with the same GSM number. In addition, in order to send an invitation to your loved ones you want to follow in the "Family" tab of the application, you have to enter their GSM numbers or select them from the contact list.

*Location data:* Your location information is processed for the purpose of showing your location on the map, showing the COVID-19 positive and risk intensity areas in your neighborhood on the map, determining your location in case of isolation, and sending you a notification in case you leave this location and informing the relevant authorities.

*Health data:* your health information is processed to determine your risk regarding COVID-19. According to the answers you give to the questions asked, you may be asked to visit the nearby health facility or follow-up questions may be directed to you about your symptoms at regular intervals.

*Occupational data:* whether you are a healthcare worker and, if you are a healthcare worker, whether you had contact with patients, is processed to determine the level of disease risk.

[35] https://hesapp.saglik.gov.tr/hayat_eve_sigar_aydinlatma.pdf.

*Transfer of Personal Data:* If you leave the area where you are supposed to be under isolation, your identity, contact and location data obtained through this application are shared with the Ministry of Interior and law enforcement officers for the purpose of protecting public health and preventing the spread of the epidemic.

## IX- EXAMINATION OF THE LIFE FITS HOME APPLICATION IN TERMS OF PROTECTION OF PERSONAL DATA AND RECOMMENDATIONS

Contact tracing applications pose a great risk because of the location data and health data that can be collected. It should be noted that the identity of individuals or communities can be revealed if location data alone is matched with three or more data. However, taking into account some minimum technologies and principles, it is possible to develop contact tracing applications without causing a privacy or personal data leak disaster. In this sense, we will mention below the principles that are technically suggested and specified in some international texts. These principles and recommendations can be found both in official texts such as the eHealth Network Text on the Use of Health Data published by the European Commission, the European Data Protection Board (EDPB) Guidelines on Applications Supporting the Fight Against COVID-19 Pandemic, and the EFF (ElectronikFrontier Foundation), and in the texts of non-governmental organizations such as EDRi (European Digital Rights) and CCC (Chaos Computer Club). Based on these texts, the arguments here have been developed.

### *1. Meaning and purpose:*

The basic premise in the use of contact and location tracing applications is the argument that contact tracing can help reduce the number of infections significantly and prominently. The validity of this assessment should be based on scientific evidence and should be under the responsibility of public health professionals. If it turns out that the person tracing through the application is not useful or the application does not fulfill its purpose, the use of the application in question should ended. The application and all data collected should only be used to combat chains of infection. Any use of the applications other than their intended purpose should be technically prevented and legally prohibited.

### *2. Volunteering and Consent:*

Due to both personal freedoms and effective public health response, users must have the power to decide and consent to participate in surveillance systems, such as an application created for virus-related location tracing. This approval should not be a prerequisite for using the applications; it should be voluntary, specific and contain detailed information, be retrievable at any time. In addition, the data collected about the user by these applications should be storable by the user, and must

be shared with the institutions with the consent and approval of the user. The importance of the application concerning the spread and speed of the disease depends on using a reliable technology that respects privacy and is voluntarily used; and not on enforced use of the application.

### *3. Transparency :*

Contact and location tracing applications are required to regularly inform users about their activities in the application. Applications must be encrypted with robust security programs and include third-party audits and leakage testing. States and governments should make public their policies concerning the application and training materials, as well as regularly publish statistics and other information on the use of each contact tracing program in the most detailed way possible. Applications must be tested and documented in terms of technical security by the chambers and non-governmental organizations as well as independent auditors who are knowledgeable about technology and privacy. The states should regularly manage and publish the results of audits made by independent experts on the effectiveness and abuse of each program.

There should be transparency about the administrative, technical and legal measures that states take. Considering the privacy interests of the persons whose personal information has been collected, governments should fully respond to their requests regarding the data collected through the programs, and an effective right of petition should be granted for complaints on this matter. Individuals should have the right to apply to the court regarding their personal data processed in these applications, when necessary. At the same time, security procedures approved by Data Protection Authorities must be applied.

### *4. Not Being Subject to Prejudice and Non-Discrimination*

Contact and location tracing applications should not be integrated with sensitive data of persons including health, gender, age, language, religion, race, ethnicity, nationality, immigration status or disability. During or after the pandemic, discrimination and labeling should not be made deliberately or otherwise based on categories, even for scientific studies. Governments have access to public health information, a set of data that should not be used for other purposes, such as application of social security laws, labor laws, criminal law or immigration laws.

### *5. Data Minimization:*

Contact and location tracing applications should collect, store and use the least amount of personal information necessary to solve the public health problem. Only the minimum data and metadata relevant and required for the application purpose (virus interaction) should be stored. For this reason, any data not specific to users' contact with the virus should not be collected centrally.

Location data does not need to match with any other data. If additional data, such as location information or health information are stored locally on phones, users should not be forced to transmit this data to third parties or even reveal them. Sensitive data such as location data, health data and ID numbers must also be securely encrypted locally on the phone. In terms of voluntary data collection for scientific research purposes, which goes beyond the purpose of real contact tracing, an explicit and separate consent must be obtained on the interface of the application and must be revocable at any time.

### *6. Duration of use and limitation of the use of recorded data:*

In contact and location tracing applications, the collection period of data collected for pandemic and isolation purposes should be stated precisely and clearly, and the data collected at the end of this period should be deleted completely. Users should have the right to request the deletion of their personal data at any time. Additional legal measures should be taken concerning the contact tracing systems for ensuring that the data collected shall not be used outside the public health context and timeframe.

### *7. Using central systems that record user data:*

Tracing people anonymously is technically possible without central servers that record all data and know everything. It is not technically necessary for user privacy to be dependent on the reliability and competence of the central infrastructure operator. The security measures promised by central systems and the reliability of the system cannot be effectively verified by users. This situation also causes ethical problems in terms of software architecture. Developing an ethical application requires the user data to remain with the user as much as possible and to have an architecture in such a way that the least data will come out. Therefore, applications and systems must be designed to guarantee the security and confidentiality of user data through encryption, anonymization, and verifiability of the source code.

No central authority should be trusted, including companies such as Google and Apple. Contact tracing and contact applications must be Free Software in terms of transparency and developability. Free Software offers sufficient transparency in order to verify complete data protection and compatible use so that a secure system can be established. Collaboration for developing global code in a secure environment can be made possible through Free Software. Solutions offered by any company or central authority will inevitably lead to countless data leaks. Free Software licenses allow for universal collaboration as well as the sharing of software code in any jurisdiction.[36] In this way, solutions developed in one country will be reusable and adopted in another country and a collective structure will thus emerge.

### *8. Designing in Line with the Privacy Policy*

A convincing level of social acceptance can be achieved when these applications are only based on privacy. User privacy should be ensured by verifiable technical measures such as cryptography and anonymization technologies. Design confidentiality principle should be adopted as an ethical principle during the development of the software. Based on this principle, users should not rely on any person or institution regarding their data in contact tracing applications.

### *9. Anonymity:*

Contact tracing IDs generated through wireless technology (e.g. Bluetooth or GPS) in applications should not be traced by third parties and should be changed frequently. For this reason, it is not appropriate to link communication data that accompany the location data such as the phone numbers, IP addresses used, device IDs, etc. with user IDs or to form user IDs with such data. The design of forming temporary user ID is possible in such a way that the identities cannot be interpreted and linked without having a user controlled private key. Therefore, temporary user IDs should not be derived directly or indirectly from information identifying users.

In addition, although it is stated that unique user IDs are created for users, this does not mean that anonymity is fully and always ensured.

The concept of *anonymity* means that your data can never be returned to be associated with a person. When your user IDs assigned by applications and systems

[36] https://fsfe.org/news/2020/news-20200402-02.en.html.

match with your other data, your data becomes pseudonymous data, that is, it does not become fully anonymous. It is possible to use a contact tracing application without collecting any personal data or creating a user ID. Therefore, it is not appropriate to derive identities for users by central systems.

## X- AN OVERLOOK TO THE "LIFE FITS HOME" APPLICATION WITH REGARDS TO MINIMUM PRIVACY PRINCIPLES AND TECHNOLOGIES

Life Fits Home (April 18, 2020) application, which was put into practice by the Ministry of Health due to the COVID-19 pandemic, has been installed by more than 10 million people in Turkey.

*Life Fits Home* Application;

The application uses the base station information received from Bluetooth, GPS and GSM operators (Turkcell, Turk Telekom, Vodafone). The application processes ID numbers, father's name and date of birth information, location data, Mernis address information, health data and telephone number of people. When this application is installed, communication (base station) data via the phone, contacts stored in the phone book, camera, photo and video, location, approximate location (network-based), exact location information (GPS and Network Based), wireless connection information, full network access information, pairing with Bluetooth devices and accessing Bluetooth settings, network connections, Google service configuration information become accessible. Personal data are processed by the Ministry of Health, and the data controller is the Ministry of Health. In addition, data is shared with the Ministry of Internal Affairs and the Police Forces, and all these institutions that share data are data controllers. Therefore, a central system has been adopted for data collection and matching, and even data exchange with more than one central database is allowed. Many personal data are collected and processed through the application that are contrary to data minimization and not relevant for public health purposes.

Users are not informed about their activities in the application, and the policies regarding the use of the application was not made public. No audit has been carried out by independent experts on the effectiveness and possible abuse of the application, and no report has been published on this issue. Transparency is not in question as it is not known what kind of administrative, technical and legal measures have been taken regarding the application and whether or not leakage tests have been carried out.

The Ministry of Health declared that the use of the application is mandatory for people who have a positive COVID-19 test and diagnosed with the disease and for people who had close contact with those diagnosed. In addition, people who have been not diagnosed can download the application from Google Play or Apple stores. When the first requested phone number data is shared by the Ministry of Health

during the installation phase of the application, the application will access your phone operator information, so your name, surname, address and other subscription information will be accessed without your approval. Therefore, the application is ethically not in accordance with the privacy principle by design, and it is not possible to determine whether an anonymous or temporary identity is generated for each user in terms of identification of users by third parties.

With the latest HES code, users' health data can be shared with private travel companies, and even users can share their health data with individuals. Sharing sensitive (private) health data of individuals with the HES code as added to the application is against the principle of data minimization, and contradicts the announced meaning and purpose of the application.

Since the Ministry of Health developed the application, the inspection of the application by independent developers and other institutions for transparency, auditability, development, detection of gaps and closing these gaps does not seem possible. It has not been clearly revealed on which scientific data and reasons the application is based before being put into use, but only the main purpose of the application was explained to be the use of processed personal data. The application is not in conformity with e-Health's Guidance on Apps Supporting the Fight against COVID-19 Pandemic in Relation to Data Protection released by the European Commission of which Turkey is a member. There is no sufficient or clear information and approval text. The data protection Guidance of the Commission also emphasizes that such applications should be subject to the supervision and control of the competent data protection authorities of the countries. There is no information or explanation about whether the application has been subjected to necessary and sufficient controls, and whether the authorized institution such as the Personal Data Protection Board has audited the application especially in terms of the protection of sensitive data including health data and other personal data.

## XI- CONCLUSION

Considering that billions of people with smartphones often use operating systems and various applications on these devices, it is possible to reach people and extract extensive data from their devices. Moreover, a continuous monitoring and surveillance is currently implemented by the hardware of smartphones (Chip, processor and antennas), operating systems (usually Apple and Google Android), application stores (Apple and Google Play), platforms (analytics companies and social media companies), and applications in accordance with informational capitalism's and platform economy's policy of adding value to data. Facebook, Google, Apple etc. and large technology companies and analytics companies have accumulated very detailed and aggregated location data for years. All data have commercial value for the platforms and generate the main source of the platform economy and create value. States obtain location data from Google, Apple, and WeChat, if they wish. We are moving rapidly towards a social, economic and political life that is transformed into data.

Technically supported "contact tracing" applications, which can make instant data tracing, are considered as a tool to prevent the spread of the COVID-19 virus in order to produce a fast and effective solution. It is considered that these applications will allow rapid monitoring of infection chains and interruption of virus interaction. In general, these applications can allow infected people and those they come into contact with to be alerted faster, so they can quarantine themselves faster and prevent further spread of the infection. However, even in this case, any corona contact tracing application is not intended to protect neither ourselves nor the people we come into contact with. It is important to note that the use of these applications will neither end the COVID-19 pandemic nor provide a solution to the global public health crisis. These applications do not lead to an end to the pandemic unless the governments take the necessary social security measures, adequate healthcare opportunities are not provided equally, and the economic concerns such as the loss of citizens' jobs are eliminated. Therefore, without taking these social and economic measures, it is not possible to find a solution to the public health crisis only through technological solutions and applications. Nevertheless, just as the public power rapidly puts technological solutions into life, more essential than that is to put social and economic measures into practice in a fair, transparent and accountable way. Therefore, this once again makes it clear that technological solutions are primarily political decisions and will.

In this sense, it is not enough to rely on the measures and promises specified by the governments in terms of technological measures and contact tracing applications. Contact tracing applications will ensure that governments have a great power of surveillance; besides, since sensitive data of individuals such as health, gender, age, language, religion, race, ethnic origin, nationality, immigration status or disability are processed, there is a serious risk of creating prejudice and discrimination in the society. Assurances concerning fundamental rights and freedoms recognized by international conventions and our Constitution in Turkey should not be removed on the grounds of public health. Wide-ranging exceptions and technological applications that would deepen surveillance should not be used to prevent the use of rights such as the right to privacy, protection of personal data and freedom of expression.

As a result of the cyber attack on 33 hospitals of the Ministry of Health in 2016, the data of nearly one million patients were stolen, and as a result of these attacks, third parties obtained not only the health information of the individuals but also other personal information.[37] A lawsuit concluded in 2018 revealed that personal data of many people, including health data, were sold by the Social Security Institution to a third company by tender.[38] Likewise, the Ministry of Health remained silent about the use of people's health data for political purposes in the 2019 local elections,[39] which is a case revealing that Turkey's Ministry of Health and other institutions cannot store personal data in a transparent and reliable manner.

Considering these negative examples, “Life Fits Home” application needs to be arranged in a transparent and auditable manner, to be in line with the recommendations of the organizations in the international conventions to which Turkey is a signatory.

[37] https://onedio.com/haber/devlet-hastanelerine-siber-saldiri-binlerce-hastanin-kayitlari-sizdi--711565.

[38] https://www.sozcu.com.tr/2018/ekonomi/skandal-sgk-hasta-bilgilerini-65-bin-tlye-satti-2225264/.

[39] https://turk-internet.com/kisitli-secmen-verileri-konusu-anayasal-koruma-altindaki-bir-hakkin-ihlalidir-ve-suctur/.


ISBN 978-605-80007-5-9