Logos Universality Mentality Education Novelty: Law
ISSN: 2284-5968 | e-ISSN: 2458-1046
Covered in: ERIH PLUS, HeinOnline, CEEOL, Index Copernicus, CrossRef, CrossCheck, J-GATE, Google Scholar, Ideas RePeC, Econpapers, Socionet, KVK, WorldCat.

2020, Volume 8, Issue 1, pages: 24-34 | doi: 10.18662/lumenlaw/8.1/33

Body Temperature - Personal Data Concerning Health. Legal Aspects in a Pandemic Approach

Ştefan Răzvan TATARU[1]

[1] PhD, Alexandru Ioan Cuza University of Iasi - Faculty of Law, razvantataru@gmail.com

Abstract: The crisis generated by the emergence of the new coronavirus and its rapid spread at global level has led states to implement measures to prevent and combat the effects of the pandemic. In the context in which the presence of the virus in the human body is manifested by the increase of body temperature, several national authorities, including the Romanian ones, imposed on public and private entities the obligation to organize their activity, so as to ensure, upon the entry of the premises, the mandatory epidemiological triage and measurement of the body temperature. In the present study, we aim at identifying and assessing the impact of the coronavirus pandemic on the personal data processing and application of the GDPR Regulation provisions. The present study highlights the types of personal data processed with the state of emergency/alert period and seeks to define whether or not the body temperature value may be included in the concept of personal data. Body temperature information is analysed by analogy with the concept of personal data, data concerning health, biological data, and sensitive or special data.

Keywords: *data protection, body temperature, data concerning health, pandemic, GDPR.*

How to cite: Tataru, Ş. R. (2020). Body Temperature - Personal Data Concerning Health. Legal Aspects in a Pandemic Approach. *Logos Universality Mentality Education Novelty: Law, 8*(1), 24-34. doi:10.18662/lumenlaw/8.1/33

1. Introduction

The emergence of the COVID-19 virus and its accelerated global spread has led to the establishment of a state of emergency in certain affected countries, the entry of public health systems on alert, and, at the same time, changes in the behaviour of individuals and economic entities. As the state of emergency caused by the pandemic may determine the prioritization of other activities over those of personal data protection, and, in order to reduce the risk of chaotic or non-compliant processing, national and European personal data protection authorities have issued several recommendations in support of data controllers. Thus, the European Data Protection Board (EDPB) has published a set of guidelines on the processing of data concerning health for scientific research purposes (European Data Protection Board, 2020a) and a set on the use of location data and contact tracing tools (European Data Protection Board, 2020b). The Romanian National Authority for the Supervision of Personal Data Processing – ANSPDCP has published a series of recommendations regarding the processing of health data in the context of the coronavirus pandemic, as well as of declaration of emergency (ANSPDCP, 2020a).

2. Personal data processing during the coronavirus pandemic

For the purpose of analysing how the state of emergency/alert caused by the coronavirus pandemic influenced the processing of personal data, we consider that it is necessary to clearly define concepts such as personal data, health data, data processing, and filling system.

According to art. 4 point 1 of the GDPR, personal data refer to "any information relating to an identified or identifiable natural person. 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".

Personal health data shall include all data relating to the health status of the data subject which reveal information about the past, the present, or future physical or mental health of the data subject (Regulation (EU) 2016/679, Art. 15 and recital No. 35).

The processing of personal data is defined in the same article as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as

collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

By the data filling system, according to art. 4 point 6 of the GDPR, we understand "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis".

3. Personal data processed during the state of emergency

The system's crisis generated by the emergence of the new coronavirus and its rapid spread globally has led states to implement measures to prevent and combat the effects of the pandemic. The measures implemented for the purpose of public health protection determined the processing of personal data of individuals who were in a certain jurisdiction or who were to enter, leave, or transit that geographical area. Most often, measures to prevent and combat the effects of the pandemic have generated processing of data relating to identity (*e.g.* name, surname, unique identifiers), location (by geolocation or statements of data subjects), itinerary, travel history, health (*e.g.* temperature), data contact (*e.g.* address, telephone number, email address), contact with persons confirmed with COVID-19 virus.

The state of emergency is a legal condition that can legitimize the restrictions of freedom, provided that these restrictions are proportionate and limited within the emergency period. Thus, the measures adopted by the controllers, during the state of emergency caused by the coronavirus pandemic, within the personal data processing activities, must respect the general principles of law and must not be irreversible (The Romanian National Supervisory Authority for Personal Data Processing, 2020b).

To the extent that it is necessary to ensure important objectives of general public interest of a Member State, such as in the field of public health, the national law applicable to the data controller may restrict, by a legislative measure, the scope of the obligations and the rights provided for within Regulation (EU) 2016/679.

4. Temperature - relevant data for identifying infected individuals

In order to reduce the spread of the virus, national authorities have put in place various measures to prevent and combat the effects of the pandemic, such as measures to prevent and control infections, the specific

conditions of application and recipients of such measures, and the public institutions and authorities implementing or monitoring the compliance and application of measures during the state of emergency/alert. In the context in which the presence of the virus in the human body is manifested by the increase of body temperature, several national authorities, including the Romanian ones, imposed on public and private entities the obligation to organize their activity, so as to ensure, upon the entry of the premises, the mandatory epidemiological triage (Law no. 55/2020, Order no. 874/81/2020, Government Decision no. 394/2020).

The obligation of epidemiological triage in order to have access the premises of public or private entities, and the processing of body temperature in an insufficiently regulated and uneven manner at the level of all controllers, provoked negative reactions from the society which considered the collection of such sensitive data as a privacy intrusion and an infringement of regulations in the field of personal data protection.

The national regulations from the Annex to Order no. 874/81/2020 details the method in which the mandatory epidemiological triage is performed. Thus, according to point II.2 of the Annex to the Order, "the epidemiological triage does not involve the recording of personal data and consists in: a) measuring the temperature by a non-contact thermometer (the recorded temperature must not exceed 37.3° C), at which may add the margin of error provided in the device leaflet".

5. Body temperature - personal data or not?

Body temperature is a personal data concerning the health status of an individual and, is characterized by volatility and temporality. The personal nature of this information results from the fact that it originates from the human body. Except for this feature, continuous temperature variations do not allow the identification of the data subject, as allowed by the human genome or papillary fingerprints (Şerban & Tataru, 2018). We conclude that the temperature of the human body does not have a distinctive character that could contribute to the identification of an individual in a group of people.

Temperature can be defined as the heat state of an environment, of a body. Some authors claim that the normal temperature of the human body is 37 degrees Celsius (Del Bene, 1990). However, other specialists consider the normal temperature of the human body as a variable concept, which depends on the place in the body where the measurement is performed. Other authors consider that the temperature varies during the day, namely,

the normal temperature in the early morning is considered to be 37.2 degrees Celsius, and the temperature in the rest of the day is considered normal in the upper limit of 37.7 degrees Celsius, a measurement performed on healthy adults aged under 40 years (Pušnik & Miklavec, 2009, p. 517).

Temperature cannot be attributed to a person in the absence of a correlation with the date and time at which it was recorded/measured, because it may present variations caused by uncontrollable factors, both internal and external to the individual (*e.g.* intense physical activity, food diet, consumption of alcohol, smoking, menstrual cycle in women, outside temperature and humidity).

The recording of the temperature, including the time at which it was measured, cannot lead to the identification of a natural person in the absence of other information, such as correlation with the video image or data relating the identity of the person. We believe that the processing of body temperature by recording it does not represent a valid personal data in the absence of recording other data leading to the identity or identification of the data subject (Oanţă, 2020).

According to the Romanian Supervisory Authority (The National Supervisory Authority For Personal Data Processing - ANSPDCP) press releases, the provisions of Regulation (EU) 2016/679 become applicable only to the extent that the information on body temperature of an identified or identifiable person are collected, registered, stored, etc. in a data filling system, according to the different means of processing" (The Romanian National Supervisory Authority for Personal Data Processing).

We consider it appropriate to analyse in detail how body temperature information can be included in the concept of personal data, taking as a reference to the definition provided by Regulation (EU) 2016/679. Next, we will analyse the information on body temperature through correlation with the four elements arising from the definition of personal data, namely: a) "any information", b) "relating to", c) "an identified or identifiable", c) "natural person" (Article 29 Data Protection Working Party, 2007).

a) The first element – "Any information"

According to the guidelines issued by the Article 29 Working Party, in order to meet the conditions imposed by the first element of the definition of personal data, such information should deliver content attributable to an individual, not showing difference whether it is correct or true (Article 29 Data Protection Working Party, 2007, p. 6). By the term "any information", the European legislator wanted to establish an extended concept of personal data (Ungureanu, 2017, p. 138), being necessary that

information directly or indirectly concerns a certain individual, regardless of its status of consumer, patient, employee, client, etc. (Article 29 Data Protection Working Party, 2007, pp. 6-7).

The experts of the Art. 29 Working Group considers that biometric data require special attention, being defined as any "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data" (Regulation (EU) 2016/679, art. 4, point 14). Biometric data is a measurable unique information, attributed to a single individual.

Body temperature is indeed a measurable information, yet it is not unique or specific to a single individual. If other biometric data such as fingerprints, retinal patterns, or facial structure can determine the precise identification of a person, the body temperature is information that can be attributed to a large number of people.

Temperature is information that fluctuates for each individual and differs from individual to individual. Moreover, temperature measurement involves variables that determine the lack of accuracy of information. The body temperature of a natural person varies between a certain minimum and maximum values that indicate a normal state of health, any deviations outside these values indicating possible medical conditions. It should be noted that the temperature measurement may be influenced by the conditions under which this information is collected (the outdoor temperature at which the measurement is performed, the activity carried out by the data subject shortly before the measurement) and the accepted error of the temperature measuring device (Pušnik & Miklavec, 2009, p. 517). Thus, in the vast majority of situations, the measured body temperature is not correct information, with an accuracy of 100%. We conclude that the principle of data accuracy (Tataru, 2020, pp. 274-275), provided in art. 5 para. (1) lit. d) of the GDPR, it becomes impossible to comply within the conditions of fluctuating, temporary personal information, difficult to measure accurately, and which is not registered in a data filling system.

b) The second element - "relating to"

According to those analysed in the Art. 29 Working Group, an essential condition for certain information to be considered personal data is the existence of an element of connection, a link between the information and the individual. Therefore, only that information concerning an individual is personal data of that person, identified or identifiable by other complementary information.

Temperature is information that can concern both individuals and goods, bodies, or environments. Temperature information cannot be clearly associated with a human being, which is why, in the absence of the link with an identified or identifiable natural person, it cannot be considered personal data.

According to an analysis by the Article 29 Working Party, "*data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated*" (Article 29 Data Protection Working Party, 2005, p. 8). In the context of the coronavirus pandemic, it is undeniable that body temperature can significantly influence the way that person is treated. For example, if the temperature of the data subject exceeds the maximum allowable limit (37.3 degrees Celsius) for entering a public institution or private entity, his/her access will be denied publicly, attracting negative social reactions from persons present. This is all the more serious as the measured data may be inaccurate, as detailed above.

c) The third element – "identified or identifiable"

The definition provided by GDPR to personal data imposes the obligation that the information concerns a natural person, identified or identifiable. We consider that a natural person is identified in the situation where it can be indicated exactly from a group or sample of people. By "identifiable person" we mean that person who has not yet been identified but who, by correlating personal data, could be identified by reducing the group.

According to art. 4 point 1 of the GDPR, "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". Thus, an identifiable person becomes identified through a process of collecting and correlating several identifying elements or fragments of information about that person.

Body temperature may represent an element specific to the physiological identity of the person concerned and, at the same time, can provide information on the person's health. At the same time, we emphasize that the identification of a person only on the basis of information on body temperature, uncorrelated with other elements of identification, is unattainable.

d) The fourth element – "natural person"

Personal data must necessarily refer to an aspect of a human being, a natural person, alive. The GDPR Regulation does not apply to deceased persons, unborn children, or legal persons. Thus, body temperature can be included in the concept of personal data as long as it is processed on living individuals.

6. Body temperature - sensitive data?

According to recital no. 51 of the GDPR, "personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms".

It is undeniable that body temperature is part of the category of health data and, implicitly, is a data of a special or sensitive nature. Special data, such as information on the health status of the data subject, may be processed by a controller under the conditions of art. 9 of the GDPR, including art. 9 lit. i), respectively the processing is necessary for reasons of public interest in the field of public health, under national law. With regard to the risks to fundamental rights and freedoms, we wonder whether controllers that perform epidemiological triage at the entrance to the entity may, through improper processing, generate considerable risks to fundamental rights and freedoms. Of course, in the context in which infection with the new coronavirus can lead to serious consequences for the health and life of any individual, public identification of people with a temperature above 37.3 degrees Celsius can lead to stigmatization of that person by those who will have access to such information. For example, the installation of video cameras with thermal scanning and the real-time display of recordings on a monitor located publicly in the area where the measurement is performed is, in our opinion, an incident to the security of personal data. Controllers must pay close attention to the processing of sensitive health data and to ensure compliance with the legal provisions on combating infection with the new coronavirus while respecting the principles imposed by the GDPR Regulation.

7. Conclusions

The measures and, implicitly, the personal data processing imposed by the state of emergency/alert do not suspend the obligations of controllers or the rights of data subjects under the GDPR Regulation. The state of emergency/alert was an unexpected test for the applicability of the GDPR

and for the maintenance of the relationship between data processing in order to pursue a general public interest and the level of the controller's interference in the data subject's privacy.

Body temperature, information frequently collected by controllers, with or without other data that identifies or could identify the person, continue to put pressure on the controller - in terms of the legality and correctness of the process in which they process information and, indirectly, on the data subject who does not understand the purpose and manner in which the data are processed, nor the relevance of incorrectly collected data, most of the time.

We consider that body temperature - the value indicated after the measurement, does not represent an authentic personal data as it cannot identify, nor contribute to the identification of a person in the absence of correlation with other personal data. The body temperature value is information on the health of the data subject, a sensitive date whose processing is of particular importance in special circumstances such as a pandemic. We conclude by stating that body temperature can be included in the concept of personal data only as a consequence of assigning it to another set of data that, regardless of the temperature value, would identify or could identify a person (e.g., 1. collecting and recording the temperature in a person's medical record; or 2. collecting and recording video images and body temperature values at the entrance to an entity).

References

Article 29 Data Protection Working Party. (2005). Working document on data protection issues related to RFID technology, 10107/05/EN, P 105, adopted on January 19th, 2005. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf

Article 29 Data Protection Working Party. (2007). Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP136, adopted on 20th June, 2007. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Del Bene, V. E. (1990). Temperature. In H. K. Walker, W. D. Hall W.D. & J. W. Hurst (Eds.), Clinical methods: The history, physical, and laboratory examinations (3rd ed.), chapter 218. https://www.ncbi.nlm.nih.gov/books/NBK331/

European Data Protection Board. (2020a). Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, adopted April 21st, 2020.

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf

European Data Protection Board. (2020b) Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted April 21st, 2020. Retrieved from: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

European Parliament, & European Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. *Official Journal of the European Union L 119/1*, 2016, May 04.

Government of Romania. (2020). Hotărâre nr. 394 din 18 mai 2020 privind declararea stării de alertă şi măsurile care se aplică pe durata acesteia pentru prevenirea şi combaterea efectelor pandemiei de COVID-19 [Government Decision no. 394 from the 18th of May 2020 on the declaration of the state of alert and the measures applied during it to prevent and combat the effects of the COVID-19 pandemic]. *Monitorul Oficial al României, 410*, 2020, May 18.

Ministry of Health, & Ministry of Internal Affairs. (2020). Ordin nr. 874/81/2020 privind instituirea obligativităţii purtării măştii de protecţie, a triajului epidemiologic şi dezinfectarea obligatorie a mâinilor pentru prevenirea contaminării cu virusul SARS-CoV-2 pe durata stării de alertă [Order no. 874/81/2020 on the establishment of the obligation to wear a protective mask, epidemiological triage and mandatory hand disinfection to prevent contamination with SARS-CoV-2 virus during the alert]. *Monitorul Oficial al României, 435*, 2020, May 22.

Oanţă, R. (2020, May 20). ANSPDCP: Doar dacă informaţiile privind temperatura unei persoane se înregistrează într-un sistem de evidenţă, legile UE privind prelucrarea datelor personale devin aplicabile [ANSPDCP: Only if a person's temperature information is recorded in a record system, EU laws on the processing of personal data become applicable]. https://www.activenews.ro/stiri-sanatate/ANSPDCP-Doar-daca-informatiile-privind-temperatura-unei-persoane-se-inregistreaza-intr-un-sistem-de-evidenta-legile-UE-privind-prelucrarea-datelor-personale-devin-aplicabile-161595

Parliament of Romania. (2020). Legea nr. 55/2020 privind unele măsuri pentru prevenirea şi combaterea efectelor pandemiei de COVID-19 [Law no. 55/2020 on some measures to prevent and combat the effects of the COVID-19 pandemic]. *Monitorul Oficial al României, 396*, 2020, May 15.

Pušnik, I., & Miklavec, A. (2009). Dilemmas in measurement of human body temperature. *Instrumentation Science and Technology, 37*(5), 516–530. https://doi.org/10.1080/10739140903149061

Romanian National Authority for the Supervision of Personal Data Processing (ANSPDCP). (2020a). Press Release – June 2020. https://www.dataprotection.ro/?page=declaratie_EDPB_iunie_2020_Covid_19&lang=ro

Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP). (2020b). Response to request no. 11010/26.05.2020 formulated by lawyer Uscov Silvia and lawyer Sava Mihaela-Ruxandra, registered in the General Register with no. 0013692 from 01.07.2020. https://legalup.ro/wp-content/uploads/2020/07/30_Ruxandra_Sava_Silvia_Uscov_11010_termoscanare.pdf

Şerban, A., & Tataru, Ş. R. (2018). The Influence of General Data Protection Regulation on patient engagement. *Logos Universality Mentality Education Novelty: Law, 6*(1), pp. 56-72. https://doi.org/10.18662/lumenlaw/07

Tataru, Ş. R. (2020). Protecţia informaţiilor de afaceri: Informaţii clasificate, confidenţiale, date cu caracter personal [Protection of business information: classified information, confidential, personal data]. *Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza" din Iaşi, Ştiinţe Juridice*, *66*(1), 274-275. http://pub.law.uaic.ro/files/articole/2020/2020_i/1.18.tataru.pdf.

Ungureanu, C. T. (2017). Protecţia datelor cu caracter personal în contractele international [Personal data protection in international contracts]. *Analele Ştiinţifice ale Universităţii Alexandru Ioan Cuza din Iaşi, Ştiinţe Juridice, 63*(2), pp. 136-154. http://pub.law.uaic.ro/files/articole/2017/volii/10.ungureanu_protectia_datelor.pdf.