NAIH/2020/2586/

Information

on processing data related to the coronavirus epidemic

Natural person data subjects as well as employers and health care professionals contacted the Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information, hereinafter: the Authority) in relation to the health care crisis due to the coronavirus (COVID-19) spreading exceedingly fast across borders inquiring about the kind of measures that can be implemented to contain the virus that are compliant with the data protection requirements in force and whether it is possible to process personal data – particularly health data which constitute a special category of personal data – in relation to the development and implementation of these measures.

Based on the queries received by the Authority, with a view to screening those possibly infected who may jeopardise the health of their colleagues even before diagnosing the disease by a physician and its treatment, certain organisations collect personal data,[1] including sensitive data[2] (health data), using questionnaires or measuring devices. Such data collections extend to trips and events outside working hours intruding upon the privacy of the data subjects; even demanding mandatory body temperature measurements for the entire staff in some places.

In view of the above, the Authority issues the following information on processing data related to the coronavirus with a view to developing compliant data processing practices by data controllers and processors, and to ensuring the efficient protection of the privacy of the data subjects. This guidance extends to organisation both in the public and the private sector and the processing of the personal data of individuals in an employment relationship or other legal relationship aimed at the performance of work and of other third persons (such as clients, visitors).[3]

1. Pursuant to the data protection rules in force, the data controller[4] – that is, the employer calling for control and the physician providing health care – carries primary responsibility for the compliance of data processing. A substantial part of data controllers, including the majority of employers, are

[1] GDPR Article 4(1): 'personal data' means 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;

[2] Privacy Act Section 3(3): "*sensitive data means all data falling in the special categories of personal data that are personal data revealing racial or ethnic origin, political opinion, religious belief or world view or trade union membership, as well as 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;*"

[3] This guidance takes into account the communications of the French and the Italian data protection authorities issued on this subject matter with a view to developing unity in the application of the data protection law.

[4] GDPR Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

required to apply the provisions of the General Data Protection Regulation (hereinafter: GDPR), excluding the bodies involved in the processing of data subject exclusively to Act CXII of 2011 *on the Right to Informational Self-Determination and on the Freedom of Information* (hereinafter: Privacy Act), thus in particular the bodies of law enforcement, defence and national security.

Just as in the course of planning any data processing, data processing including the collection, forwarding and use of sensitive personal data (health data), subject to this information, has to be developed taking into account the principles of data protection in general and the principle of accountability in particular.[5]

It is an important expectation that the processing of personal data is warranted only if and to the extent that the purpose of data processing cannot be achieved by other means not requiring data processing, and it must be examined in every case whether there are efficient solutions that pose less threat to the privacy of the data subjects. Thus, for instance, specifying basic hygienic measures, cleaning work implements and offices more thoroughly, providing disinfectants and requiring their more frequent use or regulating the order of receiving clients and using glass partitions at customer service desks may, in some cases, provide efficient solutions without the processing of personal data.

If the means referred to prove to be inadequate and the processing of personal data seems absolutely necessary, the data controller has to specify first and foremost the accurate purposes of data processing and the legal basis for compliance. The principle of data minimisation should not be left unconsidered as it stipulates that data to be processed (collected and stored) must be absolutely necessary and proportionate for the purpose to be achieved. Data controllers must also provide for the transparency of data processing as well as the accuracy and security of the data.

Pursuant to Article 13 of GDPR (and Section 16 of the Privacy Act in the case of data processing for the purposes of law enforcement, national security and defence) drawing up a privacy policy document is mandatory for all data processing purposes. The privacy policy must detail the purpose and legal basis of the data processing affecting data subjects, the period of storing the data, the range of individuals authorised to access the data in a manner that is easily understood by the data subjects; in the case of data processing based on legitimate interest [GDPR Article 6(1)f)] it is necessary to perform an interest evaluation test to verify whether the interest linked to the purpose to be achieved through data processing overrides the rights, freedoms or legitimate interests of the data subjects.

2. The Authority has identified certain requirements stemming from the legal regulation in force in relation to some frequent cases of data processing.

I. In the case of d**ata processing related to legal relationships aimed at the performance of work** (employment, the legal relationship of public employees, public servants, government employees and public service employees, as well as other legal relationships aimed at the performance of work), the employer is responsible for ensuring the conditions for the safe performance of work which do not endanger health and for planning and developing the related processes of data processing.

Under this, **the measures expected from the employer include:**

- the development of **the so-called pandemic/business continuity action plan** (hereinafter: action plan) (it is recommended that it should extend to preventive steps to be taken to reduce threats, measures to be taken upon the eventual appearance of the infection, preliminary

[5] GDPR Articles 5 and 25.

consideration of the data protection risks of the measures applied, issues of responsibility within the organisation and building efficient and adequate channels of communication facilitating the provision of information to the data subjects);
- as part of the action plan, in terms of the preliminary measures reducing threats, **a detailed information document has to be drafted and made available to the employees** concerning the most important issues to be known in relation to the coronavirus (source of the infection, mode of spreading, period of incubation, symptoms, prevention), and who to turn to in the event of any alleged contact with the coronavirus or upon the onset of other conditions specified in the information material;
- if needed, **conduct of business and business/service trips and events may eventually have to be reorganised** and the possibility of eventually working from outside the workplace must be ensured;
- attention needs to be called with emphasis to the fact that in the event of any alleged contact with the coronavirus and upon the onset of other conditions specified in the information material **individuals should report this to the designated person** and visit the company doctor or another physician immediately **in order to protect their own and their colleagues' health**.

If an employee **reports possible exposure to the employer or the employer deems that the suspicion of exposure can be established from the data provided by the employee,** the employer may record the date of the report and the personal data of the employee concerned for the establishment of their identity, the fact of whether or not the venue and date of the employee's foreign travel, even if for a private purpose, coincides with the territories (countries) and periods listed in the employer's information material; the data concerning the fact of having contact with a person arriving from the territories indicated in the employer's information material; and based on information made available to the employer, the measures taken by the employer (e.g. ensuring the possibility of visiting the company doctor, permission for a voluntary quarantine at home). **With respect to the range of data herein indicated, the Authority deems it acceptable to have the employees complete questionnaires,** if based on a preliminary risk assessment carried out by the employer in advance, the employer concludes that the application of this method is necessary and it proportionately restricts the right of employees to privacy; **however, the Authority expressly underlines that the questionnaires may not include data concerning the medical history of the data subject and the employer may not require employees to enclose health documentation.**

In such cases, **the legal basis for the processing of the data referred to above** can be legitimate interest according to GDPR Article 6(1)f); or in the case of data processing by organisations performing public tasks or exercising public powers, it may be GDPR Article 6(1)e) in view of the need to perform their basic duties. In this case and exclusively if the previous paragraph is taken into account, the fact that the condition according to GDPR Article 9(2)b) may be established for the processing of health data because the provisions of labour law require the employer to ensure healthy and safe conditions of work for the employees.

In accordance with the positions taken by the supervisory authorities of other Member States, the Authority, however, with a view to the current situation of the epidemic in Hungary, **regards disproportionate the requirement of screening tests with any diagnostic device (in particular, but not exclusively, with a thermometer) or** the introduction of mandatory measurement of body temperature generally involving all employees called for by a measure of the employer, in view of the fact that the collection and evaluation of information related to the symptoms of coronavirus and drawing conclusions from them is the task of health care professionals and authorities.

If **based on the report of an employee, or in an individual case upon consideration of all the circumstances, or on the basis of a risk assessment,** the employer finds it absolutely necessary **for certain jobs, particularly affected by exposure to the disease,** the employer can act in

compliance with the law by applying the legal basis according to GDPR Article 6(1)f) or e) (see above) as well as the conditions set forth in GDPR Article 9(2)h) and (3); thus the employer may only call for **tests to be carried out by health care professionals or under their professional responsibility** and the employer is entitled to be informed only about the results of these examinations.

II. It is important to stipulate that **health care providers as well as company doctors** – as independent data controllers – must comply with the data protection requirements governing their actions.

Besides Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data (hereinafter: Health Data Act), the legal obligation according to GDPR Article 6(1)c) and GDPR Article 9(2)i) can also be identified. This includes, for instance, Section 25 of Decree 18/1998. (VI. 3.) NM on epidemiological measures necessary to prevent infectious diseases and epidemics, which requires health care providers to report and keep records of infectious patients and persons under the suspicion of having an infectious disease, inter alia, in accordance with the case definitions specified in Annex 1 to the Decree (which also includes the SARS-coronavirus), furthermore, in accordance with the provisions of the legal regulation on the order of reporting infectious diseases and the prevention of infections related to health care[6] as well as the provisions of the Health Data Act.

In addition to the above, the procedural order related to the new coronavirus identified in 2020 drawn up by the National Public Health Centre on 2 March 2020[7] contains the epidemiological and infection control rules to be followed by attending physicians; this was compiled on the basis of the recommendations and requirements of the World Health Organisation, the European Centre for Disease Prevention and Control, hence it does not qualify as a legal regulation, nevertheless, attending physicians must apply it in the course of their activities.

III. According to the position taken by the Authority, it follows from the general requirements of conduct **applicable to employers and persons in an employment relationship aimed at performing work**, thus in particular, **the obligation to cooperate and the principles of bona fide action and fairness** that employees must inform the employer of any health or other risk affecting the workplace, other employees or third persons in contact with them in the course of performing work, including the risk of themselves being potentially infected (and also the fact of any presumed contact with an infected person).

The Authority emphasizes that in the case of data processing by the employer as described above, the employee is entitled to exercise the rights due to him as data subject in accordance with the provisions of GDPR Chapter III, the facilitation of which is the employer's obligation arising from GDPR.

IV. In relation to the processing of data related to third persons outside any legal relationship aimed at the performance of work (thus, for instance, clients and visitors), **the Authority underlines that**

- in the course of implementing enhanced control of persons entering the organisation's site and restrictions related to this as part of the **action plan** particular attention should be paid to weighing the data protection risks of the measures applied in advance and building efficient

[6] Decree 20/2009. (VI. 18.) EüM on the prevention of infections related to health care, the professional minimum conditions and the supervision of these activities

[7] https://www.nnk.gov.hu/index.php/lakossagi-tajekoztatok/koronavirus/523-eljarasrend-a-2020-evben-azonositott-uj-koronavirussal-kapcsolatban

and adequate channels of communication to facilitate the provision of information to the data subjects;

- in terms of the advance measures to reduce risks as part of the action plan, **detailed information and a notice has to be drafted and made available to third persons, which contains** the most important information related to the coronavirus (source of infection, mode of spreading, period of incubation, symptoms, prevention), together with **an appeal** addressed to them to immediately **notify the access control staff** about the fact of any presumed contact with the coronavirus or the onset of other conditions specified in the information material upon entering the site of the organisation.

According to the position taken by the Authority, the legal basis for data processing specified under Section I can also be applied to the processing of the data of third persons for this purpose as described therein.

In their action plans, organisations may regulate the measures related to these persons, which may eventually be different from rules specified for those in an employment relationship, which may necessarily be concomitant with the processing of personal data (for instance, prohibition of entry to the site of the organisation).

3. Finally, in view of the data processing interrelations, the Authority calls attention to the fact that according to Act C of 2012 on the Penal Code, the person who fails to subject himself to the epidemiological measures ordered by the competent organisation **perpetrates a criminal act**; furthermore, the criminal liability of individuals who infect someone through their wilful behaviour causing severe bodily harm or death can also be established.

In such cases, the police is entitled to take action and to process personal data pursuant to Act XXXIV of 1994 *on the Police Force*, Act XC of 2017 on Criminal Procedure and the provisions of the Privacy Act, and in the course of their actions they may also use video surveillance in public spaces in accordance with the legal requirements governing it.

Budapest, “ ” March 2020

Dr. Attila Péterfalvi
President
Honorary university professor