Guidelines on the processing of personal data in specific sectors in the context of measures against COVID-19

Following the adoption of the "*Guidelines on the protection of personal data in the context of the measures taken against COVID-19*", dated 20.03.2020, which provides important instructions for public and private controllers regarding the compliance with legal principles and criteria of personal data processing in the context of the measures against COVID-19, as well as in response to growing public interest and concern – either through media articulation, or questions raised by citizens – with respect to the specific areas of the processing of personal data (particularly the processing of health related information), the Commissioner's Office recalls by medium of these guidelines all the interested parties in relation to some practical aspects relating to the protection of personal data in specific sectors.

These aspects deal with the processing of personal data in the context of measures taken to contain the spread of COVID-19, in employment, telecommunications, health and education sectors.

On the one hand, it is deemed appropriate reiterating the fact that undeniably the processing of personal data in the fight against COVID-19 does not legitimize the restriction of the rights and freedoms of citizens exceeding the binding provisions of Article 175/2 of the Constitution.

On the other hand, the personal data protection legislation does not impede and/or restrict the rights and obligations of controllers with regard to the processing of personal data in the context of the fight against COVID-19.

Furthermore, the Office of the Commissioner wishes to emphasize that the aspects dealt with in these guidelines emanate from an appropriate interpretation of the personal data protection legislation, fully in line with the position of our EU counterparts, and the Council of Europe (CoE), as well as in the spirit of the EU regulatory framework and the CoE instruments dealing with personal data protection.

I. Processing of personal data by employers

The current crisis caused by the COVID-19 outbreak, has imposed increasing difficulties and challenges on employers vis-à-vis the processing of employees' data.

In the context of the preventive measures to contain COVID-19, several employers have decided to offer employees the option of working remotely or telecommuting[1].

Other categories of employers, due to the nature of their activity, request the presence of their employees in their regular workplaces and, in addition to the hygiene/sanitary measures and ensuring social distancing in their respective facilities, they are bound to constantly monitor employees' health conditions, so as to prevent the spread of the coronavirus.

Having said that, employees are subject to, *inter alia*, continuous checks for potential COVID-19 symptoms, and under video-surveillance monitoring about the observance of the hygiene /sanitary measures.

[1] Law No. 7961, Art. 15, "*Labor Code of the Republic of Albania*" dated 12.07.1995, as amended.

Moreover, employees working from home or telecommuting, access their employers' platforms through virtual private networks (VPNs), or use private communication channels (such as personal e-mail addresses), etc.

In this case, the Office of the Commissioner considers that employers may, in principle, process their employees' personal data (e.g. data obtained from the elevated tracking of their health), in quantity and quality which – reasonably – would exceed the normal processing of data under a normal working context.

Processing involves not only the collection and storage of processed health-related data, but also the transmission to competent bodies in charge with COVID-19 response, including, but not limited to competent authorities authorized by the law to conduct the epidemic surveillance (as provided for by the legislation on the prevention of infectious diseases).

Additionally, such processing must be conducted in accordance with the principles and criteria for personal data processing, set forth in Articles 5, 6 and 7 of the Law No. 9887, dated 10.03.*2008* "*On personal data protection*" as amended[2] ("*Law on Personal Data Protection*").

Furthermore, the use of virtual private networks (VPN), and other private communication channels for telecommuting or working from home, as well as the deployment of video surveillance systems to monitor compliance with the hygiene/sanitary rules, alongside the provisions listed above, must be associated with technical-organizational measures and strict rules, in order to guarantee data integrity and confidentiality in accordance with Articles 27 and 28 of the Law on Personal Data Protection.

To this effect, the Office of the Commissioner further urges all the data controllers to be mindful of the bylaws rendered by the Information and Data Protection Commissioner ("*the Commissioner*") in the course of their activity, particularly Instructions No. 3, 11, 22, 24, 47 and 49 of the Commissioner[3].

In this context, controllers are required to minimize any risk eventually generated by the processing of the pertinent categories of personal data under the current situation, in particular the risks threatening human dignity and privacy, and lay the groundwork regarding the return to "normal" data processing regimes (including, where appropriate, permanent deletion of the data processed in that context) once the state of natural disaster is lifted and the spread of COVID-19 is halted.

In particular, employers should not process personal data beyond what is necessary in relation to the purpose of implementing measures against COVID-19. The processing of personal data must be compatible with the purpose of the processing, and carried out as long as the processing is adequate, necessary and brings more advantages than disadvantages to achieve the purpose in question.

[2] For more details, refer to the "*Guidelines for the protection of personal data within the measures against COVID-19*", dated 20.03.2020, published on our official website: www.idp.al.
[3] The Commissioner's sublegal acts are published, as updated, on our official website at www.idp.al.

II. Transmission of location data processed in electronic communication services

One of the solutions currently being deployed in various countries around the world as part of the response to the COVID-19 pandemic is contact tracing through the transmission of individuals' location data collected by the electronic communication service providers.

The analysis of the trends of the location data is being used as a tool to help mitigate the COVID-19 crisis.

Location data means any data processed by electronic communications services, indicating the geographical position of the terminal equipment (mobile, tablet, etc.) of an electronic communications network user[4]. These data include specific information on how devices and humans move in space in time.

The Office of the Commissioner, in line with the practices and positions adopted in EU countries in this regard, as well as with the spirit of the Law on Personal Data Protection, recommends that before communicating location data, the electronic communications system providers must carry out an assessment of the impact that this type of processing has on the private lives of citizens.

Particularly important in this regard, is striking the right balance between the need leading the purpose for processing location data, in the context of measures against COVID-19, with the quantity, quality and format of these data.

Therefore, the Commissioner's Office considers that the transmission of location data performed in an aggregated and anonymous fashion aimed at, for example, to signal cases of noncompliance with social distancing, or to trace movements of individuals entering or leaving infected areas, as the need may be in the context of the measures to prevent contamination with COVID-19, or for epidemic surveillance purposes, does not constitute a violation of the provisions of the Law on Personal Data Protection and the relevant sublegal acts.

In any event the processing of the data in question must be carried out pursuant to the principles and legal criteria set out in Articles 5 and 6 of the Law on Personal Data Protection.[5]

Furthermore, the Office of the Commissioner clarifies that, in any case, the obligation to process location data in accordance with the aforementioned legal provisions does not affect the obligations of operators of electronic communications networks to act in accordance with the provisions of sectorial legislation.

Based on the practice followed so far in EU countries, the Office of the Commissioner considers that the large-scale processing of personal data can only be performed when (regardless of whether they're rendered aggregate or anonymous), on the basis of scientific evidence, the potential eventual benefits deriving in the ambit of public health benefits of such digital epidemic (e.g. contact tracking), including their accuracy, overrides (i.e., is greater than) the benefits of other alternative solutions which would be less intrusive.

---

[4] Definition according to the Article 3/56 of the Law No. 9918, dated 19.05.2008 "*On electronic communications in the Republic of Albania*" as amended.

[5] For more details, refer to the "*Guidelines for the protection of personal data within the measures against COVID-19*", dated 20.03.2020, published on our official website at www.idp.al.

While real-time information on the spread of the virus can be instrumental in isolating it, it must be stressed that, in these cases, the solutions being least intrusive in the privacy should always be the first choice.

As highlighted above, the development of these surveillance solutions should be based on a prior assessment of the likely impact of the intended data processing on the rights and fundamental freedoms of data subjects.

To such an end, the data processing should be designed and take place in such a manner as to prevent or minimize the risk of intrusion into the citizens' rights and fundamental freedoms.

III. Data processing in the context of epidemic surveillance

The Office of the Commissioner underlines that the provisions of the Law on Personal Data Protection do not hinder or limit the data processing performed in the framework of the epidemic surveillance[6] as set forth in the Law No. 15/2016, dated 10.03.2016 "*On the prevention and control of infections and infectious diseases*" ("*Law 15/2016*").

Hence, events such as the spread of COVID-19, which pose a serious threat for the health and lives of citizens, require special control measures or contact tracing in a coordinated manner, in order to identify persons who may have contacted or are exposed to the risk of infection.

The Commissioner's Office considers that the competent authorities for implementing measures for the epidemic surveillance in the fight against COVID-19 are legally authorized to process personal data and, in particular health-related data.

The processing in question includes, *inter alia*, the collection of the necessary data regarding the implementation of epidemic surveillance, the storage of such data in accordance with the applicable legal deadlines, their exchange and transmission to the bodies in question and other public and private controllers, etc.

Moreover, in the framework of the measures implemented for containment of the COVID-19 pandemic, authorities engaged in the fight against COVID-19 may have an obligation or a necessity to transfer personal data across borders to various countries and/or international organizations for statistical, scientific and/or for purposes of conducting more specialized analysis.

In this context, the Office of the Commissioner considers that the aforementioned controllers should act in accordance with the provisions contained in Articles 8 and 9 of the Law on Personal Data Protection, governing the cross border transfer of personal data.

Data processing operations for these purposes does not constitute a legitimate basis for the restriction of the individuals' rights to the protection of their personal data, as stipulated in the legislation on personal data protection.

---

[6] Pursuant to Article 3/42 of the Law 15/2016 on the "*Epidemic Surveillance*" is the systematic collection, recording, analyzing, interpreting and disseminating of the data and the analysis on infectious diseases and other related issues on regular basis, to gain insights about the disease, its spread and to take measures to eliminate, eradicate, control and prevent it.

As mentioned above, the provisions of Articles 5, 6 and 7 of the Law on Personal Data Protection, as well as the bylaws of the Commissioner (especially Instruction No. 49) apply in this case as well.

Furthermore, it is worth noting that the anonymization of data as a measure to protect privacy in the context of epidemic surveillance, does not automatically lead to a restriction of the right to the protection of personal data, under the excuse that this right hinders or is in contrast with the epidemic surveillance purposes. Anonymized data are also explicitly covered by the provisions of the Law on Personal Data Protection[7].

This rule applies also to the processing of location data dealt with in paragraph II.

IV. Data processing in the education sector

As is widely known, due to the measures against COVID-19, pre-university and university education institutions have not halted their educational work, but have carried on through online platforms, where personal data are processed (including recorded images) of pupils, students and professors.

Accordingly, when considering the technical solutions aimed at ensuring the continuity of the educational activity, data protection-oriented standard configurations should be preferred, for instance regarding the default settings, so that the usage of applications and software does not infringe the rights of the data subjects (pupils, students, professors) and to avoid processing more data than necessary to achieve the legitimate purpose of ensuring educational continuity, in accordance with Article 5 of the Law on Personal Data Protection.

It is also of primary importance that a proper legal basis is chosen for the data processing (as defined in Article 6 of the Law on Personal Data Protection), especially when children are involved, where the Commissioner's Office urges controllers to obtain parents' approval of legal guardian where necessary for the intended data processing in the context of online learning.

The aforementioned requirement must be further accompanied with the provision of a thorough (and as exhaustive as possible) information to the parents or legal custodians of the children, about all aspects related to the processing of children's data, pursuant to the provisions of article 18 of the Law on Personal Data Protection.

In each case dealt with in these guidelines, the Office of the Commissioner emphasizes that the processing of data in the education sector in the context of social distancing must be carried out in accordance with the provisions of the applicable legislation in force both in the personal data protection and the sector-specific fields.

***

The Commissioner's Office will continue to provide guidance for the public and private controllers, as well as for the data subjects, on an adequate interpretation and application of

[7] Article 3/3 of the Law on Personal Data Protection

the Law on Personal Data Protection, in the context of the measures against COVID-19, having in focus the protection of citizens' life, health and, obviously, personal data.

The safety of our fellow citizens remains our ultimate priority.