Date: 30 March 2020
Title: Opinion on the legal basis for data collection in relation to COVID-19
Number: 07120-1/2020/25
Legal act: Opinion

The Information Commissioner (hereinafter the IC) received your request for opinion on the assistance that Jožef Stefan Institute (hereinafter the Institute) offered to the Government of the Republic of Slovenia, namely the assistance in creating a temporary information system that will enable the analysis of non-personal and anonymized data in the field of health service, financial and economic flows, electronic communications, public service, traffic, transport and other services that appear to be related to the planning and implementation of the COVID-19 epidemic control measures. You explained that the purpose of this system is to enable the Government to better assess the current situation, to forecast the developments of the COVID-19 epidemic, and to prepare the ground for action to contain the COVID-19 epidemic.

You drafted a proposal for a Government decision and an agreement between the Ministry of Defence (MoD), Ministry of Health (MoH) and the Institute and you request the IC to issue an opinion on the legal basis for data collection. Data that is intended to be collected is non-personal and anonymized data received from health care providers, the Financial Administration of the Republic of Slovenia, electronic communications operators and others. Data originators will provide data on a voluntary basis. This will include location data, although such data will only be processed for statistical purposes, e.g. to monitor whether the COVID-19 related measures are complied with and for analysing population movements, with a view to monitoring daily migration within and outside Slovenia (Article 3, paragraph 4 of the Agreement), in such form as, for example, "45 persons with an Italian operator's mobile number passed checkpoints between 8 AM and 10 PM".

You enquire whether data originators need a legal basis for transmitting such data to the Institute and whether the Parties to the Agreement (MoD, MoH and the Institute) need a legal basis for statistical analysis and analytical evaluation of such data. In addition, you would like to know whether an emergency law is necessary in case state authorities want to use this location data for different purposes (e.g. tracking groups of people)?

On the basis of the information you provided and having regard to Article 58 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter the GDPR) and point 7, first paragraph of Article 49 of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 94/07, official consolidated text, hereinafter ZVOP-1), and Article 2 of the Information Commissioner Act (Official Gazette of the Republic of Slovenia, No. 113/05, hereinafter ZInfP), the IC hereby provides its non-binding opinion with regard to your question.

As a preliminary remark, the IC observes that there is a clear need for effective coronavirus epidemic control measures, however this situation should not be used to restrict fundamental human rights and freedoms. The IC points out that the measures envisaged must be effective and necessary in the context of what is reasonable in a democratic society. The IC understands that certain anonymous data may significantly help to better plan and implement epidemic control measures, but special diligence should be used in understanding the notion of anonymization. Using anonymous data should

take precedence over the use of personal data, especially with regard to location, communication and health data of individuals. Interferences with individuals' information and communication privacy are inadmissible in a democratic society if aims pursued can be achieved with effectively anonymized data, and such interferences must be in accordance with the Constitution of the Republic of Slovenia.

The key legal question with regard to the legal basis for processing of personal data is whether personal data is being processed or not. The Decision attached to your letter offers only a very general description of the intended data processing and the types of data intended to be processed. Notwithstanding the assurances you gave, namely that only anonymized data will be used, the Information Commissioner considers that most likely at least some categories of data will be difficult to transmit into the intended system and be processed in a manner that ensures processing of anonymous data. The IC sets out hereafter its detailed concerns, especially regarding the communication and location data potentially acquired from the electronic communications operators. The IC believes that it is difficult to achieve anonymization standards for this type of data so that no legal basis would be needed for its processing. The IC especially warns of the risk of anonymisation processes whereby the identification of individuals may occur when data which is deemed anonymised from different originators is combined into a large database. Such a data set allows new links between the data, making individuals identifiable, in particular when such sets include communication location data and traffic data. If it is impossible to assert (with an appropriate statistical certainty) that data used in the intended processing is anonymous, the IC underlines that an appropriate legal basis is required. In addition, the controller is obliged to precisely establish the data set which is to be processed and to determine the purposes for processing, while also complying with the basic principles of processing, including the principle of proportionality, and implementing other obligations laid down in the GDPR (including the data protection impact assessment as referred to in Article 35 of the GDPR). However, with regard to communication traffic and location data, the IC warns that such data is protected in accordance with Article 37 of the Constitution of the Republic of Slovenia. Below we explain our concerns in more detail.

1. Processing of anonymized data from different originators

The documentation we received does not provide information on which data from individual originators are intended to be used. However, judging from the contents of the proposed Government Decision and the Agreement, we find that the data set referred to in Article 3, paragraphs 3 and 5, of the Agreement is most likely not personal data, as data refers to the sales and stock of business entities engaged in trade in food, fuel and medicine; that is, of course, if no data on buyers as natural persons will be processed, but only data on the situation with regard to sales and stock. Similarly, no personal data is processed when processing information on healthcare providers or pharmacies referred to in paragraph 1 of the Agreement if they in fact include only statistical, non-personal and anonymized data on the daily consumption of resources or medicines or the overall assessment of medical conditions in relation to the COVID-19 epidemic and not to individuals' health data. If such information can be directly or indirectly linked to identifiable natural person, even if this can only be performed by a third party and not by the controller itself (as we explain below), such data is personal data or - depending on the source - sensitive personal data.

Special caution should be exercised with regard to data referred to in Article 3, paragraph 4 of the Agreement, which stipulates that the data of electronic communications operators referred to in the first paragraph of the said Article shall refer to such non-personal data that demonstrate the daily

amount or frequency of electronic communication in specific locations and such data that enable the analysis of population movements with the purpose of establishing daily migration within and outside of Slovenia.

This data cannot be obtained without processing source personal data from the electronic communications traffic and such processing (meaning anonymization) can only be performed by entities that have a legal basis. This means that anonymization should be carried out by the operators themselves and they should hand over to the Institute or other entities only anonymized data and in no way personal data. Special attention in this regard should be drawn to the restrictions laid down in Article 151, paragraph 5 of the Electronic Communications Act (ZEKom-1) regarding the processing of traffic data, which defines a specific set of persons who are entitled to process data, under the control of an operator, for specific purposes only. This particular provision falls within the scope of the Agency for Communication Networks and Services. Thus, the Institute is not allowed to perform anonymisation on its own; individuals' traffic and location data must be anonymised by the originator. If the Institute processed personal data for the purpose of anonymization on behalf of and on documented instructions of the operator this could be considered contractual processing in accordance with Article 28 of the GDPR. In addition, data processed for the purpose of anonymization should not be used for other purposes, as this would be in contravention of the purpose limitation principle and would breach the GDPR and the ZEKom-1.

The IC cannot infer from the attached materials any specific assurances as to the fact that only anonymized data will be transferred from the operators to the new information system, since it is not even defined which databases of the operators and which methods of anonymisation will be used in the process of anonymization. The IC explains below in more detail what is meant by anonymized data, namely data from which individual cannot be identified directly or indirectly.

In the light of the foregoing, the IC emphasizes, in particular, the inadequacy of the provisions of Article 4, paragraphs 1 and 2, and of Article 5, paragraphs 1 and 2 of the Agreement. The reason for this, as already mentioned, is that the Institute alone does not have a legal basis for performing any sort of anonymization processes or other processing of personal data from the originators. Such processing can be performed only by the originators of data themselves, that is, if their sectoral legislation does not restrict it.

The IC proposes, in addition, to **include explicit safeguards** in the Agreement, by which it is prohibited to process data which is not actually anonymized by anyone other than the originators, and to specify the duty of the users to immediately inform the originators if they receive data from which individuals could be identified, and to destroy such data that they received.

2. Identifiability of individuals and the legal basis for the processing of traffic and location data

If it is impossible to assert (with an appropriate statistical certainty) that data used in the intended processing is anonymous, the IC underlines that appropriate legal basis is required for entities that are not originators and/or when processing is performed outside the originators' legitimate purposes for processing. The legal basis should also contain the principle of proportionality in the narrow and broad sense and specify the purposes of processing, the subjects involved, the datasets and the duration of processing, as well as other conditions as set out in the Constitution of the Republic of Slovenia, as explained below.

The IC hereby draws special attention to the correct understanding of the notion of identifiability of the individual. Personal data relate to identifiable individuals, but it is important to know that the relevant question we need to ask ourselves here is "whether it is possible to identify individuals from the data" and not "whether *we* are able to identify them." The notion of identifiability should be understood broadly; is it possible to identify individuals, do other entities have knowledge, capabilities and data that may lead to the identification of individuals, etc. At the same time, particular caution is necessary with smaller groups of people (e.g. less than 5 individuals), especially when it comes to location and communication data (!), as identifiability of individuals increases significantly here. Anonymization processes should also take into account the risk that the identification of individuals occurs when data from different originators that is deemed appropriately anonymised is combined into a large database. A data set allows new links between the data, making individuals identifiable, in particular when such sets include communication location data and traffic data.

The IC also emphasises the need to differentiate between encrypted and anonymized data - proper encryption prevents unauthorized persons from becoming aware of the content, but it does not mean that data becomes non-personal and that identification is no longer possible. Encrypted personal data is pseudonymised personal data and is thus still personal data (see Article 4, point 5 of the GDPR); it is not anonymous data. Processing of only pseudonymised personal data thus also requires an appropriate legal basis. The use of one-way hash functions or encryption algorithms does not mean that source data can never be restored. This is particularly possible if we know what type of data the source data was, and even more so if the source data is particularly structured, such as the personal identification number or tax ID number. The same personal identification number will always generate the same encrypted value. On the other hand, identifying source data is much more difficult if we do not know the structure of the input data (whether it was a number, a word, longer text, an image). If unauthorized persons obtain pseudonymized personal data, it is the same as if they obtained raw personal data, it will only take slightly longer to identify the individuals. Truly anonymous data is only obtained through the use of specific anonymization methods and techniques (such as noise addition, permutation, differential privacy, aggregation, K-anonymity, L-diversity and T-similarity) and not simply by encoding, encryption or other types of 1:1 mirroring.

The EDPB Opinion on Anonymization Techniques may be of assistance in understanding anonymization techniques and is available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

The IC recommends that you inform the originators and the Institute with these guidelines, if they are not already familiar with them, so that they are properly observed.

The IC also points out that certain questions cannot be answered or discovered without making individuals identifiable.

Potential questions to operators include, but are not limited to: "Where are specific infected individuals located or how are they moving?", "Was person A at t-time at location z or in the vicinity of person B?"," Which individuals were located at location x at t-time?" and the like. Acquiring such data, which is undoubtedly personal data, means an interference with constitutionally protected databases of electronic communication traffic data. Any such interference and giving answers to such questions is considered interference with both communication and information privacy of individuals, regardless of whether the answer is affirmative or negative. Such questions cannot be answered without

interferences mentioned above and without processing of personal data. This means that the operators are required to have an adequate legal basis for the processing of the mass data of their users. Within the current legal framework, the Information Commissioner sees no legal basis for that in the context of measures you mention, namely measures related to the COVID-19 epidemic. **It should be borne in mind that this is an interference with the constitutionally protected communication privacy enshrined in Article 37 of the Constitution of the Republic of Slovenia. This provision stipulates that interference with privacy of communication is only possible if all constitutional conditions are met cumulatively:**

(1) only a law may prescribe that,
(2) on the basis of a court order
(3) the protection of the privacy of correspondence and other means of communication and the inviolability of personal privacy be suspended for a set time
(4) where such is necessary for the institution or course of criminal proceedings or for reasons of national security.

***

In conclusion, the IC stresses the urgency of limiting the proposed processing to (effectively) anonymised data. In the case at hand, however, there is reasonable doubt that this is feasible with regard to the purposes you laid forth.

If processing of anonymised data is impossible to ensure, there should be an appropriate legal basis for the processing. Should new legal basis be created for processing of data, held by electronic communications operators, such a basis should be valid only for the duration of the epidemic declared. This is particularly important because electronic communications traffic data and personal data are constitutionally protected in accordance with Articles 37 and 38 of the Constitution of the Republic of Slovenia, and any interferences with these rights must be limited to what is necessary in a democratic society. Emergency measures in such exceptional situations should not be used as a mechanism to interfere with fundamental human rights.

Yours faithfully

Mojca Prelesnik, LL.B.,
Information Commissioner

Prepared by:
Andrej Tomšič, M.A.
Deputy Information Commissioner