Deliberation 2020-061 of June 11, 2020Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Friday July 03, 2020NOR: CNIX2016896XDeliberation n° 2020-061 of June 11, 2020 providing an opinion on a draft decree setting the list of organizations or services responsible for a public service mission that may implement the processing of personal data for the purpose of responding to a health alert, under the conditions defined in Article 67 of Law No. 78-17 of January 6, 1978 relating to data processing, files and freedoms (request for opinion no. 20007810) The National Commission for Data Processing and Freedoms,

Seizure by the Minister of Solidarity and Health of a request for an opinion concerning a draft order issued for the application of Article 67 of Law No. 78-17 of January 6, 1978 relating to data processing, files and freedoms;

Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

Having regard to the public health code;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 67;

Having regard to decree n° 2019-536 of May 29, 2019 taken for the application of law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its article 67;

Having regard to Decree No. 2019-341 of April 19, 2019 relating to the implementation of processing involving the use of the registration number in the national identification directory of natural persons or requiring consultation of this directory, in particular its article 2 B (10°); After having heard Mrs. Valérie PEUGEOT, Commissioner in her report, Mrs. Nacima BELKACEM, Government Commissioner, in her observations, Issues the following opinion: The provisions of Article 67 of the Data Protection Act provide that the processing carried out by certain data controllers - the bodies or services charged with a public service mission listed in the draft decree -, and having the sole purpose of responding, in the event of an emergency, to a health alert and to manage its consequences, are subject only to the provisions of section 3 of chapter IV of regulation (EU) 2016/679 of 27 April 2016 (GDPR). The provisions of section 3 of chapter III of title II of the Data Protection Act relating to prior

formalities with the CNIL are therefore not applicable to them, by way of derogation from its article 66.

The draft decree also has the effect of allowing organizations and services responsible for a public service mission relating to the management and follow-up of health alerts to process the registration number in the national identification directory of natural persons , pursuant to Article 2 B (10°) of Decree No. 2019-341 of April 19, 2019 relating to the implementation of processing involving the use of the registration number in the national identification directory of natural persons (NIR) or requiring the consultation of this directory.

The Commission emphasizes that the derogatory regime provided for in Article 67 of the Data Protection Act, which is intended to apply to each health alert and not only to the management of the health crisis linked to covid-19, must subject to strict interpretation.

It also recalls the obligation for the data controllers concerned to ensure compliance, on the one hand, with the basic rules set out in section 3 of chapter III of title II of the law (conditions of information and rights of individuals, etc.) and, on the other hand, the principles laid down by the Public Health Code, in particular its article L. 1110-4. On the data controllers who could benefit from this derogation

The draft decree is intended to establish the list of data controllers who can benefit from the system mentioned in article 67 of the law.

The Commission considers, firstly, that the bodies or services charged with a public service mission acting as a subcontractor or as a recipient within the meaning of Article 4 of the GDPR are not intended to be included in the draft decree.

It thus considers, taking into account, on the one hand, the missions attributed to certain actors by the legislative and regulatory texts and, on the other hand, the information transmitted by the Ministry, that certain bodies such as regional health observatories or even the organizations and services responsible for reporting information or implementing data processing (Digital Health Agency, Health Data Platform, Technical Agency for Information on Hospitalization) do not seem to act as of processing manager. They should therefore not appear in the decree.

Secondly, and in addition, should only appear on the list of bodies vested, in application of a legislative or regulatory text or in compliance with the missions entrusted by the competent authorities, the mission of responding to a health alert or to manage the consequences in the event of an emergency.

In this respect, the Commission wonders about the hypotheses in which certain organizations appearing in the draft could be

required to implement, as data controller, processing operations whose sole purpose is to respond, in the event of a situation of emergency, to a health alert and to manage the consequences, with regard to:

- regional health observatories;

- organizations and services whose purpose is research in the field of health or contributing to such research;

- departmental directorates for social cohesion and the protection of individuals;

- the Digital Health Agency;

- the Health Data Platform;

- the Technical Hospital Information Agency. mission, for example, to participate in the management of a health alert in order to implement such processing. This was particularly the case with the Institut Pasteur as part of the COVID-TELE project.

The Commission takes note of the ministry's commitment to replace, in the draft decree, the research teams of the hospital centers by the university hospital centres, the research projects involving the processing of patient and/or staff data being carried out under the responsibility of the head of establishment. On the purposes pursued by the processing

According to the Ministry's analysis, the scope of application of the derogation provided for in Article 67 of the law would apply to all processing operations covered by section 3 of the law.

The Commission would like to point out that the sole purpose of the processing benefiting from this derogation must be to respond, in the event of an emergency, to a health alert and to manage the consequences […] .

Firstly, the processing thus implemented must not provide for sub-purposes that do not meet all of the criteria mentioned. For example, should be excluded from the scope of the derogation processing for the purpose of setting up warehouses to enable subsequent processing to be carried out.

Secondly, the Commission notes that the notion of health alert is not defined in the legislative or regulatory texts. When this derogation was introduced into the Data Protection Act by Act No. 2016-41 on the modernization of our health system, the impact study of the bill thus specified the notion of health alert in the framework of this system: the health alert relates to any new and abnormal phenomenon or event presenting a short or medium term risk for public health, whatever its nature, requiring implementation as soon as possible measures to reduce this risk.

These provisions also refer expressly to the missions of the National Public Health Agency (ANSP, or Public Health France, formerly the National Institute for Health Surveillance), which is responsible in particular for preparing for and responding to

threats, alerts and health crises. and launching the health alert (articles L. 1413-1 et seq. of the public health code). According to a 2005 report by the working group of the Institute for Health Monitoring, health alerts can come from two sources: health indicators collected routinely and reflecting the state of health of an individual or a population , or an environmental exposure to a dangerous agent , or an event of any nature and origin associated with a threat to public health .

The Commission considers that the processing can only be implemented within the framework of a health alert launched by the ANSP, in accordance with the provisions of Articles 67 of the Data Protection Act and L. 1413-1-6° of the Code public health, both in terms of managing the response to the alert and managing its aftermath. Thus, the organizations and services listed in the draft decree will not be able to carry out the assessment of the health alert situation themselves.

Thirdly, the Commission considers that a restrictive approach to the notion of emergency situation should be adopted, limiting the implementation of this system to situations of serious health threat calling for emergency measures as defined to Article L. 3131-1 of the Public Health Code and to the state of health emergency as defined in Article L. 3131-12 of the Public Health Code. It also considers that the organizations will have to interpret the notion of emergency situation in accordance with the settled case law of the competent courts.

In this respect, the Commission draws the Ministry's attention to the fact that a number of projects recently submitted for authorization and linked to covid-19, which constitutes an example of a health alert, do not fulfill, according to the analysis above, the criteria set out in Article 67 of the law. This applies in particular to several research projects which, although carried out during the state of health emergency, did not directly aim to provide, in an emergency situation, responses to the health crisis.On the categories of data processed

Given the sensitivity of the data processed, the Commission calls for the greatest vigilance in respecting the principle of data minimization and the criteria linked to the purposes of the processing implemented in the derogatory framework laid down by article 67 of the law. Computing and Freedom .

In addition, in the event that the processing of data from the health data system (SNDS) is envisaged, the Commission recalls that the provisions relating to the SNDS (Articles L. 1461-1 et seq. of the Public Health Code) provide for specific procedures for the implementation of the processing of the data it contains (in particular compliance with the security reference system and, apart from the permanent access authorized by the legislator, the communication by the data controller to the Platform of the data of health of a certain number of elements which must then be the subject of a publication).

Thus, while article 67 of the Data Protection Act exempts the data controller from an authorization, it does not however aim to derogate from the other provisions of the public health code relating to the SNDS, which remain fully applicable.

Finally, the Commission recalls that the data processed must be relevant to the purposes of the processing, and that compliance with the principle of data minimization must lead to the collection of only the data strictly necessary for the purposes pursued. Thus, it considers in particular that the processing implemented by the services of the departments within the framework of this system should be strictly limited to their geographical competences. On the processing of the NIR and the associated security measures

The Commission stresses that the draft decree also aims to establish the list of bodies and services entrusted with a public service mission in charge of the management and follow-up of health alerts, as provided for by the provisions of the article 2 B (10°) of decree n° 2019-341 of April 19, 2019.

Firstly, the Commission recalls that Article 86 of Decree No. 2019-536 of May 29, 2019 adopted for the application of Law No. 78-17 of January 6, 1978 relating to data processing, files and Libertés specifies that, in accordance with the principle of minimization, the NIR can be processed within the framework of this system when such use constitutes the only means of collecting personal health data necessary to deal with the health emergency. In particular, the Commission wonders about the possibility for certain players listed in the draft order to process the NIR that has not been the subject of a cryptographic operation, even though this processing is not provided for in within the framework of the missions traditionally assigned to them. In application of the principle of minimization, the NIR should only be processed in its literal form when it is absolutely necessary for the fulfillment of the purposes, which the data controller must expressly justify, for example in the context of the analysis of data. impact on data protection. When the NIR is only used to allow the pairing of data between two sets of data, only a NIR that has previously been the subject of cryptographic operations replacing it with a meaningless code should be able to be processed. . In the absence of clarification on this point in the draft, the Commission takes note of the ministry's commitment to specify in the decree that the organizations mentioned in 8° of the draft text will not be authorized to process the NIR in the situations referred to in Article 67 of the Data Protection Act. However, it invites the Ministry to specify explicitly in the decree, with regard to the other organizations mentioned, whether the NIR that they will be able to process must have previously been the subject of cryptographic operations.

Secondly, the Commission recalls that this processing can therefore only be carried out in compliance, on the one hand, with

Articles 5-1-f and 32 of the GDPR and, on the other hand, with Article 86 of the aforementioned decree. Thus, any processing of the NIR must be carried out under very high-level security conditions, given the risks associated with the processing of this data. The encryption measures implemented must therefore comply with the state of the art and the general security reference system published by the National Agency for the Security of Information Systems. On the performance of the impact analysis relating to data protection

The Commission notes that Article 67 of the Data Protection Act subjects the processing it is intended to regulate to the sole provisions of Section 3 of Chapter IV of the GDPR which concerns the impact analysis relating to data protection. (DPIA) and the prior consultation of the supervisory authority when the DPIA indicates that the processing would present a high risk if the data controller did not take measures to mitigate the risk (Articles 35 and 36 of the GDPR).

Under the terms of Article 35 of the GDPR, a DPIA must be carried out prior to the implementation of the processing when the latter by the use of new technologies, and taking into account the nature, the scope, the context and the purposes of the processing is likely to create a high risk for the rights and freedoms of natural persons.

In accordance with deliberation no. 2018-327 of October 11, 2018 adopting the list of types of processing operations for which a DPIA is required, this is particularly the case of processing for the purpose of managing alerts and reports in social and health issues. In addition, the Commission points out that such a DPIA is required when this processing meets at least two of the nine criteria resulting from the guidelines of the European Data Protection Board (EDPB) on the impact assessment relating to the protection of data (collection of sensitive data, processing of data concerning vulnerable people, large-scale data processing, crossing or combining of data sets, innovative use, etc.).

The Commission therefore considers that each processing that will be implemented within the framework of Article 67 of the Data Protection Act must, except in duly justified exceptions, have previously been the subject of a DPIA.

In addition, the Commission considers that it is up to the controller to document, both in the DPIA and in its register of processing activities, that the processing envisaged complies with the conditions provided for in Article 67 of the Data Protection Act. .On the procedures for carrying out the Commission's missions on the processing implemented

The Commission notes that the derogations governed by the first paragraph of Article 67 of the Data Protection Act expire one year after the creation of the processing.

Consequently, if the processing continues to be implemented beyond this period, this must be the subject of a formality in

accordance with the provisions of article 66 of the Data Protection Act. With regard to research not involving the human person which does not comply with a reference methodology, the authorization procedure provided for in article 76 of the Data Protection Act must be respected; in particular, the file must be submitted to the Health Data Platform and examined by the Ethics and Scientific Committee for research, studies and evaluations in the field of health.

The Commission draws the attention of the Ministry and the data controllers concerned to the fact that it will not be able, at the end of the one-year period, to authorize the continued implementation of processing which does not comply with the provisions of the GDPR and the law and could, therefore, also order the data controller to erase the data collected.

In addition, the Commission remains competent to exercise its powers of control and prescription of corrective measures or sanctions.

Finally, the Commission draws the Ministry's attention to the fact that, within the framework of the procedure for examining by its services applications for authorization relating to projects linked to covid-19, each of the projects has object, within a very short time, of a consequent accompaniment in order to allow the delivery of an authorization. Above all, this support has enabled the data controllers concerned, in the majority of cases, to modify the projects presented in order to comply with the principles relating to the processing of personal data or the provisions of the Public Health Code. In addition, it recalls that nearly a third of research projects not involving humans related to covid-19 have been the subject of reserved or unfavorable opinions from the Expert Committee for Research, Studies and evaluations in the field of health, most often due to methodological shortcomings or difficulties. On the implementation of additional safeguards by data controllers

The Commission points out that the transparency of processing is one of the cornerstones of the assessment of the public interest.

The Commission considers it desirable that data controllers inform it as far in advance as possible of the processing carried out. This information will also enable it, where appropriate, to support data controllers and help them better define the conditions for implementing their processing.

The Commission also wishes to be made the recipient of the list of processing operations carried out within the framework of Article 67 of the Data Protection Act. Following the example of the doctrine that it has established in terms of single decisions, it asks that the data controllers concerned send it an annual report containing in particular the list of processing implemented in this context as well as the methodology followed.

It also insists on the need to implement guarantees of transparency of processing vis-à-vis the data subjects, and in particular compliance with the information procedures provided for in Article 13 of the GDPR and Article 69 of the Computing and Freedoms or, where applicable, Article 14 of the GDPR, leading to the implementation of appropriate measures to protect the rights, freedoms and legitimate interests of the persons concerned, in the event that it is envisaged to apply the provisions of Article 14-5-b of the GDPR, such as collective information channels.

The president,

M. L. Denis