Deliberation 2021-081 of July 8, 2021Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Saturday August 20, 2022NOR: CNIX2219623VDeliberation No. 2021-081 of July 8, 2021 providing an opinion on a draft decree relating to the information system for the unique identification of victims (SIVIC) (Request for opinion no. 21004242)The National Commission for Computing and Liberties,Request by the Minister for Solidarity and Health of a request for an opinion on a draft decree relating to the unique victim identification information system (SIVIC);

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 (General Data Protection Regulation);

Having regard to Article L. 3131-9-1 of the Public Health Code (CSP);

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms (data-processing law and freedoms);

After having heard the report of Mrs Valérie PEUGEOT, commissioner, and the observations of Mr Benjamin TOUZANNE, government commissioner, Issues the following opinion: unique identification of victims amending the provisions of decree no. 2018-175 of March 9, 2018, codified in the public health code. This processing, called SIVIC and for which the minister responsible for health is responsible, is provided for by article L. 3131-39-1 of the CSP, aims, in the event of an event constituting an exceptional health situation or being likely to involve many victims, particularly in the event of collective accidents, to ensure the management of these events and the monitoring of victims. Article L. 3131-9-1 of the CSP refers to a decree in Council of State, taken after opinion of the Commission, the care to specify the nature of the data collected and to fix the methods of their transmission in the respect of the rules guaranteeing the protection of the private life.On the purpose of the treatmentThe draft article R. 3131-10- 1 of the CSP details the purposes of SIVIC, which do not appear in Decree No. 2018-175 of March 9, 2018. The Commission welcomes this modification, which it considers likely to promote compliance with the principle of transparency. nature of the data processedThe draft article R. 3131-10-2 of the CSP details the categories of personal data that will be recorded in SIVIC and which relate to three categories of people: the people taken care of, the people to contact in order to inform them of the care of a relative (contact persons) and the users of the information system. With regard to the persons covered: The identification number of the persons in the national directory for the identification of natural persons as a national health identifier ( NIR INS) is added to the categories of data collected, in particular to improve identity monitoring and to detect any duplicates. Although the Commission understands this objective, it nevertheless notes that this processing is likely to concern a large number of people, in particular in the event that the device is used in the context of a major event. The Commission also notes that the draft text submitted to it is a Conseil d'Etat decree, with a level of standard enabling the cases of use of the NIR to be extended. However, this modification results in providing for the use of the NIR outside the cases provided for by 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. natural persons or requiring the consultation of this directory (NIR framework decree). She also wonders about the legal basis allowing the collection of the NIR INS in SIVIC. Indeed, it recalls that the processing of this data is governed in particular by the provisions of Articles L. 1111-8-1 and R. 1111-8-1 and following of the CSP, Article 30 of the Data Protection Act, as well as by the NIR framework decree. In this respect, it specifies that the referencing using the national health identifier must be carried out, according to the terms of article R. 1111-8-3 of the Article 2-B-1° of the aforementioned decree, by professionals, establishments, services and organizations mentioned in Article L. 1110-4 and professionals forming a care team pursuant to Article L. 1110- 12 and intervening in the health or medico-social care of the person concerned. However, the Commission notes that these categories do not include the ministry responsible for health, designated as data controller, as well as most persons referred to in draft article R. 3131-10-3, such as, for example, personnel under the ministries home, justice and foreign affairs eras. It also notes that the draft article R. 3131-10-3-V° provides for the transmission of the NIR INS in the information system set up to organize the exchanges defined in article 10-6 of the code of criminal proceedings, which are not part of the health or medico-social care of the persons concerned. In this respect, and as it has had occasion to do in its previous opinions, the Commission draws the attention of the Ministry on the risks generated in terms of privacy by the substantial increase in the number of organizations and people required to process the NIR in this context and on the imperative need to confine the use of the NIR INS to the health and medical spheres -social under the conditions provided for by the public health code. It therefore invites the Ministry to clarify the project on this point, particularly with regard to the legal qualification of the NIR used in SIVIC.

According to the details of the ministry, the recording of data will be carried out only by the administrative staff of the health establishments. Health professionals can only provide them with additional information. The Commission draws the Ministry's attention to the fact that the details of the different categories of data collected within the framework of SIVIC (weight, state of consciousness, type and institution of hospitalization, certificate of clinical care, etc.) as well as the context of their collection necessarily involve the processing of personal health data, within the meaning of Article 4-15) of the General Data Protection Regulation ( GDPR). As such, it takes note that the Ministry undertakes to exercise particular vigilance with regard to the methods of collecting this information and to raise awareness among the people informing SIVIC, in particular with regard to the free comment areas. or notepads, likely to contain irrelevant data. With regard to users: Concerning the collection of the mobile telephone number of users of the information system, provided for by draft article R. 3131-10-2 2 ., the Commission notes, as it did in its deliberation No. 2017-322 of December 7, 2017, that this will in principle be the user's professional telephone number. It also notes that in the event that the professional does not have a professional mobile telephone number, the collection of a personal number cannot be imposed on him. The Commission notes that the Ministry has undertaken to remove the adverb in particular from the draft article, so that an exhaustive list of data that is adequate, relevant and limited to that necessary is drawn up. On the retention period for data The draft decree does not mention the retention period for data that will be contained in SIVIC. According to the details of the ministry, the data concerning the persons supported and the contact persons are kept for a period of two years from the closing of the event, at the end of which the data will be deleted. Log data relating to system usage will be retained for one year after the event is closed before being deleted. Additionally, as directed by the Ministry, in the event of events involving only pick-ups medico-psychological, the closing of the event will take place thirty days after the opening of the event. Otherwise, an event is closed no later than thirty days after the last patient has left the hospital or until the end of the complete hospitalization of the last patient of the event. Asked about the criteria for the end of hospitalization, the ministry specified that the follow-up of hospitalization must include follow-up and rehabilitation care, as well as hospitalizations in psychiatry at the end of treatment in a department of medicine, surgery or obstetrics. Furthermore, the Commission notes that the closure of an event is not definitive because, according to the details of the Ministry, an event could be reopened at the initiative of the regional health agencies (ARS) or the general management of the (DGS), when a person has to be rehospitalized after the end of the event. Therefore, the Commission invites the Ministry to clearly specify in the draft decree the criteria and methods for calculating the duration of data retention. The Commission notes that the data of SIVIC users will be kept until the closure of the user account. The Commission invites the Ministry to modify the draft decree in order to indicate the retention period of the data, for each category of persons concerned. On the recipients of the data Article L. 3131-9-1 of the CSP provides that SIVIC data may be transmitted for the purpose of managing the event and monitoring victims, to designated agents within regional health agencies and competent ministries. Draft article R. 3131-10-3, however, provides for the transmission of SIVIC data to the National Public Health Agency (ANSP), during events of an epidemic or biological nature, recipient not mentioned in article L. 3131-9-1 of the CSP. T While noting that the ministry has undertaken to modify the draft decree so that only pseudonymised data is transmitted to the ANSP, the Commission wonders whether the draft could provide for such transmission. Moreover, the Commission recalls, in the event that SIVIC should be interconnected with other information systems, that such reconciliations would require modifying the draft decree as well as the texts governing their implementation and that the categories of recipients must comply with the texts in force and in particular article L. 3131-9-1 of the CSP. Finally, the communication of data is likely to lead to the extension of the retention period for SIVIC data, which does not seem to be provided for by the texts.On the information of personsThe Commission invites the Ministry to include in the draft decree the procedures for informing persons whose data are intended to be processed in s SIVIC. In addition, given the sensitivity of the data concerned, and because of the context justifying its implementation, the Commission considers it necessary that, in accordance with Article 12 of the GDPR, the Ministry publishes on its website concise, transparent information , understandable and easily accessible, in clear and simple terms so that the entire population can be aware of the existence of SIVIC and understand its scope and interconnections.Concerning the people supported:According to the details of the ministry, the persons covered will be informed of the processing of personal data concerning them within the framework of SIVIC by the delivery of a certificate at the end of a somatic or medico-psychological treatment. The Committee wonders about the temporality of the information: the outcome of a medico-psychological treatment that can occur within a variable time after the occurrence of the event and, consequently, the recording of the data in SIVIC. It invites the Ministry to provide information to the people taken care of prior to their registration in SIVIC and, in the event that the people are not in a condition to receive this information, to inform them as soon as their condition allows it. The Commission takes note of the fact that the Ministry recommends that establishments inform the family or the trusted friend of the persons taken into care during their possible visit. More generally, the Commission recalls that according to the terms of the article 12 of the GDPR, the information provided must be concise, transparent, understandable and easily accessible, in clear and simple terms. It insists, in view of the situation of particular vulnerability in which the persons concerned by the processing find themselves, on the need to take the greatest account of these principles. Thus, having read the model information document, the Commission: notes that it mentions that SIVIC does not involve the processing of medical data. The

Commission considers that this statement is likely to call into question the correct understanding of the processing envisaged, the latter relating to data concerning health; invites the Ministry to modify the information relating to the duration of data retention in the certificate in order to to avoid a reference to the regulatory provisions of the CSP.

The Commission notes that the Ministry has undertaken to specify therein the limitation of the rights of data subjects, in accordance with Article 23.2.h of the GDPR.Concerning contact persons:The Ministry has not specified how the contact persons will be informed of the processing in SIVIC of the personal data concerning them. The Commission notes that the Ministry has undertaken to provide individual information to contact persons and to communicate to them a document containing all the information provided for by the GDPR. Concerning SIVIC users: According to the details of the Ministry, users are informed of the processing of personal data concerning them through SIVIC's general conditions of use (CGU) which will be displayed and validated by the user during their first connection and after each update of the CGU. The Commission notes that the information is not limited to the display of the T&Cs and is supplemented by information available on a dedicated page available on the SIVIC portal to which users can refer throughout the duration of the processing.On rights access, rectification and opposition of persons The draft article R. 3131-10-4 excludes the exercise of the right of opposition and does not mention the right of erasure of the persons concerned by SIVIC. According to the details of the ministry, the right of erasure and opposition cannot be exercised because of the objective of SIVIC. The Commission analyzes these exclusions as the mobilization of the provisions of article 23 of the RGPD which make it possible to limit the rights of individuals in order to guarantee, in particular, important objectives of public interest in the field of public health. The Commission notes that the Ministry has undertaken to modify the draft decree so that it mentions the reasons for which the rights of individuals are limited as well as the risks for the rights and freedoms that the processing presents, in accordance with Article 23.2.g of the GDPR. According to the details of the ministry, the rights of individuals may be exercised with the DGS and, for people in care, with the health establishment or the medical emergency unit. - psychological bearer of the information provided in the tool. The Commission notes that the Ministry has undertaken to supplement the draft decree accordingly. On data security and traceability of actions The planned processing, carried out on a large scale and including in particular sensitive data, has been subject to a data protection impact assessment and has undergone a security accreditation before it goes into production. Due to the sensitivity of the data contained in SIVIC, the hosting of its services will be carried out by an outsourced service provider certified as a health data host (HDS). Encryption measures to ensure the integrity and confidentiality of the data processed will be put in place as part of the processing, both concerning storage, both access flows and data exchanges. The technical mechanisms implemented for these measures comply with the state of the art, and in particular with the recommendations of the general security reference system (RGS); sensitive data, including the NIR INS, will be encrypted at rest in the database and during backups, by state-of-the-art algorithms using encryption boxes. Compartmentalization of data using cryptographic methods is also planned to reduce the risk of re-identification of patients. Concerning the authorization of persons who can access the processed data, an authorization matrix has been produced in order to manage access as need and according to authorization profiles allowing granularity of access. Concerning the authentication of authorized users, different authentication methods are available within SIVIC: strong authentication by CPx card, strong two-factor authentication by password single-use password and simple authentication by password in accordance with deliberation no. 2017-012 of January 19, 2017 adopting a recommendation relating to passwords. Features related to account management require the use of strong authentication. Access to SIVIC business data requires either authentication by password, or authentication by CPx card if it has been previously registered in SIVIC. The Commission notes that recommendations relating to authentication by CPx card will be communicated to users during their training and are part of the documentation associated with the tool, but recalls its recommendation to secure access to health data through strong authentication with two factors. Concerning the authentication of authorized users in accordance with the National Health Identifier (INS) reference system, suitability tests will be carried out and validated by the national filing and approval center (CNDA) in order to ensure that the good suitability of SIVIC with the INSi teleservice. The projected processing will be subject to self-approval in order to be able to call this teleservice via a connection authenticated by server certificate. In this context, the Commission notes that the teleservice will only be called upon the voluntary and manual action of the user via a button in the SIVIC file and that such a call will only be made during an operation research by patient identity traits. It also acknowledges that functional traces will be put in place including the user, the structure, the date and time of the call to the teleservice and recalls the need for monitoring and reporting of alerts related to this functionality. .Concerning the export functionalities linked to an event within a health establishment, SAMU or ARS, the Commission notes the implementation of a limitation of the data extracted to what is strictly necessary to respect the right to know about it. authorized users and authorizations set up for each profile, as well as functional traces showing the author, date and time of extraction. It notes that the Ministry has undertaken to put in place an awareness message during each extraction and recalls the need for monitoring and reporting of alerts related to this functionality presenting a significant residual risk.

Pseudonymized data may be exported within the framework of the management of events of an epidemic or biological nature in accordance with the missions of alert and health monitoring to the services of the Ministry of Health as well as to the ANSP. The Commission acknowledges that no identity data will be present in these exports and that work is in progress to hash the SINUS number using a state-of-the-art cryptographic hash function and a salt hash generated using a key stored in an encryption box. The exports will then be encrypted and transmitted to the recipients via secure protocols. Regarding the availability of the data, a disaster recovery plan will be implemented and the backups will be replicated on a geographically distant secondary site. The retention period of the functional traces is set at two years after the end of the event. The Ministry justifies this duration by the need to monitor and ensure access to authorized persons in the context of their missions, as well as to be able to use these traces in the context of legal requisitions. The Commission specifies, however, that the starting point of the retention period, which may be very far from the date of generation of the record, and the retention period itself do not comply with its usual recommendations, which are to keep functional traces for a maximum period of one year from the generation of the functional trace. It recalls that control procedures must be implemented on a regular basis in order to identify unauthorized access and must give rise, if necessary, to the establishment of a data breach report within a reasonable time. It notes that the technical traces, including data on the use of the service by its users, will be kept for a period of one year from the end of the event. It therefore asks to reduce the retention period of functional traces to what is strictly necessary and to choose a fixed period, with a rolling expiry date for the retention periods of functional and technical traces, or to provide specific justification demonstrating a high risk for the data subjects who need to keep these traces beyond the recommended duration, in particular in the event of the possibility of misuse of the purpose of the processing. The Commission recalls that, in the event that SIVIC is interfaced with other processing, no database should collect all the information collected in each of the interconnected processing operations and that data transmissions should be secured by state-of-the-art algorithms and protocols. It recalls that adequate security and minimization measures should be put in place in order to reduce the risks associated with this type of transmission. Finally, the Commission notes that an operational security center will collect and analyze the traces and events produced by the SIVIC software, servers and network equipment as well as the various security services. Here again, it recommends that the application traces and events collected and analyzed be kept for a period consistent with its recommendations. Regarding the data collected by this operational center, the ministry clarified that these traces will not include health data or directly nominative data of patients and users. The Commission takes note of this. The

President,

M.-L. Denis