

Deliberation 2021-048 of April 15, 2021 Commission Nationale de l'Informatique et des Libertés Nature of the deliberation:

Opinion Legal status: In force Date of publication on Légifrance: Thursday September 16, 2021 NOR:

CNIX2124319SDeliberation No. 2021-048 of April 15, 2021 providing an opinion on draft decree in Council of State creating an automated processing of personal data called "interministerial information system for victims of attacks and disasters" (SIVAC) and amending the code of criminal procedure (request for opinion n° 21001458) The National Commission for Computing and Liberties, Seizure by the Ministry of Justice of a request for an opinion concerning a draft decree in Council of State creating an automated processing of data at personal character referred to as the interministerial information system for victims of attacks and disasters (SIVAC) and amending the code of criminal procedure; 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 the Code of Criminal Procedure, in particular its article 10-6; Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms; After having heard the report of Mrs. Christine MAUGÜÉ, commissioner, and the observations of Mr. Benjamin TOUZANNE, government commissioner, Issues the following opinion: The draft decree submitted for opinion to the National Commission for Computing and Liberties (hereinafter the Commission) aims to create a processing of personal data known as the interministerial information system for victims of attacks and disasters (SIVAC). The purpose of this processing is to allow different actors to exchange the information necessary to help the victims of attacks or disasters in order to improve the conditions of their care and their follow-up. On the scope and conditions general rules for implementing the system Firstly, the Commission notes that Article 10-6 of the Code of Criminal Procedure (CPP) provides that the administrations, within the meaning of Article L. 100-3 of the Code of Relations between the public and the administration (CRPA), intervening in the management of the crisis, the care of the victims of these events, their accompaniment or the implementation of their rights, the public prosecutor's offices and the courts in charge of the procedure as well as approved victim support associations within the meaning of the last paragraph of article 41 of the CPP may exchange between them the data, information or documents strictly necessary for the conduct of these missions as well as for the information of the persons present. nts at the scene of the events and their loved ones. The Ministry has indicated that it interprets the expression crisis management broadly and considers that these exchanges must allow and facilitate the appropriate care of all those present and their relatives. Article 1 of the draft decree specifies that SIVAC processing will

therefore concern events occurring on the territory of the French Republic or those which, occurring outside the territory, involve French nationals and foreign persons residing regularly in France. The Commission observes that the interministerial information system SIVAC will be powered by flows from partner applications involved in counting, identification assistance, support and information missions for victims and their relatives. These applications are as follows: SINUS (standardized digital information system), SIVIC (unique victim identification system managed by the Ministry of Health), Crisenet and CriseCIAV (which is to be replaced by an interministerial information of the public and assistance to victims (C2IPAV) managed by the Ministry of the Interior) for any type of event; the software of the guarantee fund for victims of acts of terrorism and other offenses (FGTI) as well as the application IPG de France victims in the context of a terrorist act. It notes that the planned device only includes information flows from partner applications to SIVAC and that no transmission of information from SIVAC to the Partner applications will only be possible. In general, it recalls that the various aforementioned processing operations must, where applicable, be modified in order to expressly provide for the transmission of personal data to the SIVAC processing operation. The Commission thus emphasizes that the SIVAC processing is intended to centralize many data, some of which may be particularly sensitive, such as the registration number of persons in the national identification register of natural persons (NIR). It recalls, with regard to the volume of data likely to be processed and their nature, that appropriate legal and technical measures must be provided for in order to ensure a high level of protection for them. Secondly, with regard to scope of SIVAC processing, the Commission notes that it will be activated: once the competent authority considers that the usual means may not be sufficient to ensure correct management of the event and proper handling of the victims, which will result in the use of partner applications (and not from a threshold which would be determined according to the number of victims); manually under the authority of the national anti-terrorist prosecution (PNAT) or the center crisis and support from the Ministry for Europe and Foreign Affairs during terrorist events. While the scope of the planned system appears broad, it takes note of the Ministry's details that the supply of SIVAC will be done in two stages. Initially, this processing will be fed by information concerning the existence of events managed by partner applications but will not contain personal data relating to persons registered in these applications. Apart from the particular case of events linked to terrorist acts for which SIVAC can be triggered directly by manual entry under the authority of the national anti-terrorist prosecutor's office (PNAT) or the crisis and support center of the Ministry for Europe and of Foreign Affairs, it is only in a second step that the transmission of the personal data of the persons concerned to SIVAC can be carried out. The Commission notes that this transmission will then be

subject to the decision of the competent authority (public prosecutor's office or, in cases where a disaster does not require an investigation by the public prosecutor's office, an information unit activated for crises) to resort to this processing for the event in question. On the applicable legal regime and the purposes of the planned processing : information, support, implementation of rights and thus falls under 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 (GDPR). In this respect, the Commission also notes that the data recorded in SIVAC will not be used to allow cross-checking for the purposes of criminal prosecution. Under these conditions, the Commission considers that the intended purposes are determined, explicit and legitimate in accordance in article 4-2° of the law of January 6, 1978 as amended. On the data collected Article 1 of the draft decree provides for the categories of personal data and information likely to be recorded in the processing according to the categories of persons concerned: the persons sought and the persons having made contact with the information units, the persons present or declared at the scene of the event and their relatives as well as the victims and their relatives, and those accessing the treatment. As a preliminary point, the Commission observes that the notion of relatives is used both in 2° (persons present or declared on the premises x of the event and their relatives) and 3° (victims and their relatives) of draft article R2-15-1. It takes note that, in the context of 3° of this provision, the concept of relatives can also refer to indirect victims. In this respect, it therefore wonders about the scope of this notion and considers that it should be specified in the draft decree, in particular if 2° and 3° of article R2-15-1 of the draft decree are not intended to target the same categories of persons. Firstly, the Commission notes that, with regard to persons present or declared at the scene of the event and their relatives as well as victims and their relatives, In particular, administrative data relating to the type of health care, including medico-psychological, may be collected from the SIVIC application. With regard to the nature of the data collected in the context of SIVAC processing, the Commission notes that, according to the Ministry, the planned processing does not include so-called sensitive data within the meaning of the GDPR. Asked about this point, the Ministry considers in particular that no data concerning the health of the persons treated is collected and that only administrative data is collected and processed. The Commission observes that it is specified by recital 35 of the GDPR that personal data relating to health should include all data relating to the state of health of a data subject which reveals information about the past, present or future physical or mental state of the data subject. concerned person . The Commission notes that several pieces of information recorded in SIVAC are likely to reveal, in certain cases, information on the state of physical or mental health of persons (the date of treatment by the health establishment, the hospital

of destination, care by a CUMP, the name and address of the current hospital, the hospital status, the fact that the person is unconscious or the hospital status). It also observes that, in the category of data relating to the rights of victims, the degree of invalidity attributed according to the scale of the pensions sub-directorate of the Ministry of the Armed Forces may be collected. Under these conditions, the Commission considers that data relating to health are collected and processed within the framework of SIVAC. It invites the Ministry to clarify the draft decree and the impact analysis relating to data protection (AIPD) in this sense and takes note of its commitment on this point. It also considers that the Ministry will have to draw all the consequences of the presence of such data in SIVAC with regard to access to this sensitive data. Secondly, the Commission therefore draws the Ministry's attention to the articulation of the transmission information to SIVAC by partner applications with medical secrecy, as protected by Article L. 1110-4 of the Public Health Code, in particular for the data that will be transmitted by SIVIC and SINUS and access to this data recognized in SIVAC to certain personnel, even if they are bound by professional secrecy, other than the authorized professionals who take care of the persons concerned. In this respect, the Commission recalls that under this provision, information collected by a health establishment, during an act of prevention, diagnosis or treatment is protected by professional secrecy and that only a legal derogation from this rule, authorizes a professional to access data covered by medical secrecy. In view of these elements, if it notes that Article L. 3131-9-1 of the Public Health Code provides for the transmission of such data to the agents designated within the regional health agencies and the competent ministries for the purpose of ensure the management of the event as well as the follow-up of the victims, it considers that it will be up to the ministry to ensure that the personnel not covered by the above article who may have knowledge of the data covered by medical secrecy have the right to know about it. Thirdly, the Commission observes that the draft decree provides for the collection of assigned identifiers, including the NIR, for victims and their relatives. The Commission observes first of all that the various identifiers which may be collected in SIVAC, including the NIR, can only be accessed by actors who strictly have the right to know about it in the context of their missions and cannot be accessed by all SIVAC users. In addition, it recalls that the specificities of the NIR, and in particular its significant character, justify that the use of this identifier remains strictly regulated by the law of January 6, 1978 as amended and limited to the purposes for which its use is permitted under the terms 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 or requiring consultation of this directory. The Commission notes that the health insurance funds, family allowance funds, the pensions sub-directorate of

the Ministry of the Armed Forces, employers of personnel from the intervention forces who are injured or deceased as well as the FGTI, which may already have knowledge of the NIR under of Decree No. 2019-341 mentioned above, wish to be able to use the NIR as part of SIVAC processing in order to identify the individuals involved in the events s mentioned in article 10-6 of the CPP. It also acknowledges that the NIR can only be processed by these players within the framework of SIVAC. In view of these elements, the Commission wonders about the planned use of the NIR for the relatives of the victims. It recalls, in any case, that the use of the NIR in SIVAC can only be done in accordance with the aforementioned decree n° 2019-341 and that, failing this and in the absence of modification of this decree framework, the NIR cannot be processed and notes that a modification of the decree is envisaged in this regard. The Commission also notes that other identifiers may be collected, namely the identifier assigned to the person in the application of origin, the identifier assigned to the person concerned in SIVAC, or even his tax number. On this point, it notes that the collection of the tax number will only concern persons who are victims of acts of terrorism and considers that this could usefully be clarified in the draft decree. It notes that the tax number will enable the Directorate General of Public Finances (DGFIP) to communicate it to the Departmental Directorates of Public Finances (DDFiP), in addition to the identity and contact details of the persons concerned, in order to avoid any risk of homonyms and allow the victims to be located in all the departments where they are taxed. It also acknowledges that only the DGFIP and the DDFiPs may have knowledge of this tax number. In view of the foregoing, while the Commission observes that there may thus be simultaneous collection and use of the tax number and NIR of the persons concerned in SIVAC , it notes however that these two numbers will be sectorised in the processing and will not will not be accessible by the same actors, who need either the NIR or this tax number in order in particular to allow certain identification of the person in charge. The other categories of data do not call for observation on the part of the Commission. Under these conditions, the Commission considers that the data processed are adequate, relevant and not excessive with regard to the purposes pursued. On accessors and recipients Article 1 of the draft decree lists the accessors and recipients of SIVAC processing according to the nature of the data recorded in this processing and their need to know. In general, the Commission notes that SIVA C will not be used by the operators of the information cells brought, within the framework of this type of event, to inform the relatives of a victim. It also takes note of the details provided by the Ministry, namely that the total number of people accessing treatment will be around seven thousand and that access will be opened up gradually, over several years depending on the priorities set and in order to allow a correct increase in load and the realization of the possibly necessary adjustments. As regards the recipients of the

personal data contained in SIVAC , the Commission notes that these will be the one hundred and one departmental directorates of the general directorate of public finances for victims of terrorist acts as well as the administrative foreign countries carrying out the same missions for their nationals. Given the above and the particularly large number of accessors and recipients of processing data, the Commission draws the attention of the Ministry to the need to manage with the greatest vigilance the authorizations of personnel who can access the processing and be recipients of the data it contains. Although it acknowledges the implementation of different authorization profiles, it generally considers that consideration should be given to the need to make all of these personnel accessing the processing or recipients of all or part of the data it contains, in order to regulate this access more strictly in order to limit the risks. graces (DACG) will have a user account that only allows access to the statistical data produced. It notes that this department will only be able to access aggregated data which no longer contains personal data and that, for this reason, it is not mentioned in the draft decree as accessors to the processing .On data retention periods Draft Article R2-15-3 of the CPP specifies the retention periods for data recorded in SIVAC processing, which may be between six months and thirty years. The Commission notes that these retention periods have been determined taking into account the limitation periods and the legal durations linked to the rights of victims. In any case, it also notes that, in the event that a person can no longer benefit from the status of victim because he is qualified as an alleged perpetrator, a decision of the authority concerned may lead to the early deletion of the data relating to this person in the processing. In addition, the Commission notes that it appears from the information transmitted by the Ministry that pseudonymised data may be kept for a period of fifteen years after the date of the event in order to allow the display of homogeneous statistics over this period. As this retention period does not appear in the draft decree submitted to it for its opinion, it asks that it be supplemented and takes note of the ministry's commitment on this point. Under these conditions, the Commission considers that the data retention periods provided for by the draft decree are not excessive.On the rights of individualsAs a preliminary point, in general, the Commission wonders about the articulation of the rights of the persons concerned as provided for in SIVAC with the terms to exercise the rights of these same persons determined within the framework of partner applications. It considers that a reflection should be carried out on this point for consistency purposes. Firstly, with regard to the information of the persons concerned, the Commission notes that the Ministry wished to adapt the methods of information to the situation experienced by the persons concerned by favoring information in stages. Thus, the information notices that will be given to the people concerned by the partner applications as well as the letters sent by the service of access to law and justice and assistance to

victims (SADJAV) of the Ministry of Justice will mention the existence of SIVAC as well as the procedures for exercising the rights and the web address where to find all the other information provided for in Article 14 of the GDPR. The Commission notes that the possible transfers of data for foreign nationals will be indicated in the information notices published on the website of the Ministry of Justice. In this respect, for the purposes of transparency for the persons concerned, it considers that these information notices should be supplemented in order to specify the reason of public interest that the ministry intends to mobilize under article 49-1.d.) of the GDPR to justify these transfers. It takes note of the ministry's commitment on this point. Given the fact that SIVAC processing is likely to concern foreign nationals, it considers that it could be useful to provide these mentions of information in several languages. Secondly, the Commission observes that the right to object provided for in Article 21 of the GDPR is set aside by the draft decree on the basis of Article 23-1.i) of the GDPR with regard to the processing of personal data of certain persons (persons sought and having made contact with the information units, persons present or declared at the scene of the event and their relatives , victims and their relatives) by authorized personnel of the Ministry of Justice and of the investigation service or of the unit for the identification of victims of disasters contacted, when the purpose of this transmission or this consultation is to guarantee the protection of people. However, it notes that data subjects may object to the communication of their personal data to other partners. Thirdly, the Commission notes that the rights of access, rectification, opposition and limitation of the processing provided for by Articles 15 to 18 and 21 of the GDPR are exercised with the service in charge of victim assistance within the secretariat of the Ministry of Justice, which does not call for observation. On transfers The draft decree indicates that transfers of personal data may be made to foreign administrations carrying out the same missions for their nationals, including those of countries not on the list provided for in Article 45 of Regulation (EU) 2016 /679 of the European Parliament and of the Council of 27 April 2016 when an important reason of public interest so requires, in accordance with Article 49.1 of the same regulation. The Commission takes note that ad foreign ministries which may benefit from such data transfers are the consular services of foreign countries competent for French territory, which are sometimes provided by the embassy. It notes that, in the absence of a decision of adequacy under the article 45, paragraph 3 or appropriate guarantees under article 46, a transfer of data to the foreign administrations concerned may be carried out on the basis of article 49-1.d) of the GDPR. In this respect, the Commission notes that the Vienna Convention on Consular Relations of 24 April 1963, to which France is a signatory, requires in particular in its Article 37 that consular posts be kept informed of certain situations concerning their nationals by the competent authorities. of the State of

residence (death, guardianship or curatorship, shipwreck and air accident). As regards the countries which are not signatories to this convention with which France maintains bilateral relations, the Commission notes that they generally have consular representation in France and that a transfer of data concerning their nationals is likely to be carried out on the same basis. In view of these elements, the Commission recommends the adoption of additional measures to guarantee the security and confidentiality of personal data. personnel of the persons concerned during these transfers. On the security measures The Commission takes note of the precise ions made by the Ministry concerning the technical solutions used to ensure the security and traceability of data. It notes that access to personal data, which is only permitted to persons who need to know through an authorization management system and the associated management processes, complies with the expected level of security. The Commission observes that the access accounts are opened after the user has been trained and has signed the user charter and that a review of access rights is carried out at least once a year. It notes that the training in the use of the tool also provides for raising awareness of the protection of personal data. data from the Ministry of Justice and is not subcontracted. factorial. It notes that the Ministry confirms the implementation of encryption solutions in accordance with the requirements of the RGS. With regard to traceability, the Commission notes the implementation of an escalation of alerts established from the events dreaded devices allowing rapid reaction to any anomaly. The other security measures do not call for comments from the Commission. However, it recalls that the security requirements provided for in Article 57 of the amended law of 6 January 1978 require the updating of the AIPD and its security measures with regard to the regular reassessment of the risks. President Marie-Laure DENIS