Deliberation 2021-133 of November 18, 2021Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Saturday March 12, 2022NOR: CNIX2207710VDeliberation n° 2021-133 of November 18, 2021 providing an opinion on a draft decree creating an automated processing of personal data called "digital support platform for victims" (request for opinion no. within a request for an opinion concerning a draft decree creating an automated processing of personal data called "digital platform to support victims"; Having regard to Directive 2016/680 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 by competent authorities for the purposes of the prevention and detection of crime criminal proceedings, investigations and prosecutions in this area or the execution of criminal penalties, and the free movement of such data; Considering the modified law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms; On the proposal of Mrs. Sophie LAMBREMON, commissioner, and after having heard the observations of Mr. Benjamin TOUZANNE, government commissioner , Issues the following opinion: The National Commission for Computing and Liberties (hereinafter, the Commission) has been asked by the Ministry of the Interior for an opinion on a draft decree creating an automated processing of personal data referred to as the "digital support platform for victims" (hereinafter, the PNAV). The purpose of this processing is to allow people who believe they are victims or witnesses of offenses involving attacks on persons to be directed to personnel of the national police or specially trained soldiers of the national gendarmerie and to exchange in real time, with the latter, from an electronic means of communication. The PNAV is intended to replace the platform for reporting sexual and gender-based violence, on which the Commission ruled in its deliberation n ° 2018-310 of September 13, 2018. At the request of the Commission, the implementation of this treatment was the subject of an assessment after a first year of use. This evaluation made it possible to highlight the important role, particularly in times of health crisis, of the platform in reporting domestic violence, and thereby to assess the need to extend the system to other offenses requiring individualized support. With this in mind, the creation of the PNAV aims to cover, beyond sexual and sexist offences, a series of offenses against persons - such as attacks on physical integrity or mental state of the person or harm to minors and the family. Although it covers a wider perimeter than the platform for reporting sexual and gender-based violence, the planned system essentially takes up the architecture of the latter. Thus, the PNAV will be accessible via the "service-public.fr" site, which will host instant discussion channels (chat). As soon as it appears, during a conversation, that the facts reported are related to the purposes of the PNAV and require legal treatment, the conversation will be entered into

professional software (for the national police, the "new computerized handrail" or N-MCI; for the national gendarmerie, the "national gendarmerie procedures drafting software" or LRPGN) with a view to its transmission to the competent investigation services. If the Commission does not question the general economy of the system nor the need to create such processing, it nevertheless issues a few observations on some of the conditions for implementing the PNAV.- On the one hand, it observes that exchanges between declarants and operators will initially be carried out via a web platform but that the ministry does not rule out using other means of electronic communication likely to raise new issues. n of the PNAV and N-MCI processing raises legal difficulties, in particular with regard to the categories of data processed. - Finally, with regard to the security of the processing, the Commission notes that the planned system involves the storage of data by service providers does not make it possible to ensure a sufficient level of guarantee. As long as the processing is carried out for the purposes of prevention, investigation and prosecution of criminal offences, it falls within the scope of the Directive (EU) 2016/680 of April 27, 2016 referred to above and must be examined with regard to the provisions of Titles I and III of the law of January 6, 1978 as amended. Insofar as the processing is likely to relate to data mentioned in I of article 6 of the law of January 6, 1978 as amended, it must be the subject of a decree in Council of State, taken after reasoned and published opinion of the Commission, in accordance with article 89 of this same law .On the purposes and function nment of the processing Article 1 of the draft decree provides that the purpose of the processing is to enable a person who considers himself to be a victim or a witness of one of the offenses listed to enter into contact and to exchange with a staff of the national police or a member of the national gendarmerie and to make a report from an electronic communication network. In this perspective, the processing allows the agents of the platform to inform the declarant of his rights, to direct him to the competent services and associations for his accompaniment, to facilitate his reception and his care by the police services and gendarmerie, or to collect and transmit reports to the territorially competent investigation services. With regard to the means planned to achieve these ends, the Commission observes firstly that the exchanges between a declarant and a national police personnel or a soldier of the national gendarmerie will take place "from an electronic communication network" but that, however, the draft decree does not specify the means of communication that can be used. The Commission notes that initially, the exchanges will be carried out from a teleservice made available to victims and witnesses on the "service-public.fr" site. It also observes that the ministry plans to extend the means ensuring exchanges, for example by allowing the use of SMS. However, the use of other means of communication is likely to raise new issues, particularly relating to the confidentiality of exchanges. As regards the use of SMS,

the Commission recognizes the relevance of such a means in certain circumstances, and in particular in the case where a declarant does not have internet access. However, the data exchanged in this way may not be deleted, automatically or by the operator, from the declarant's telephone. If, moreover, the ministry has provided several functionalities limiting the risks of discovery of use of the web platform by third parties, like a button allowing to leave and quickly erase the conversation, these functionalities do not may be applied to exchanges carried out by SMS. In general, the Commission considers that the scope of offenses covered by the platform as well as the vulnerability of the victims call for favoring means of communication that can be accompanied by guarantees relating to the confidentiality of the exchanges of on the one hand, and to the deletion of the data as soon as possible on the other hand. be informed and, where appropriate, seized of any new electronic communication functionality. In the same way, it underlines that the impact analysis relating to data protection (DPIA) sent to it must be updated before using such a feature, in order to take into account the risks for the people concerned and identify the measures to mitigate them. one of the offenses covered by the draft decree. The ministry has not ruled out that reports concerning the same person may be reconciled even if, given the retention period of the data (four hours), such reconciliations seem difficult. However, the Commission questions the need to reconcile such reports with regard to the purposes of the processing. Indeed, the purpose of the PNAV is not to allow the judicial processing of a report but aims to facilitate, upstream of a possible judicial investigation, the exchanges between a declarant and the services of the police or the national gendarmerie. . In this sense, any reconciliation between reports is not necessary for the purposes of the processing and is intended to be carried out in a second stage, once a report has been transmitted to the competent investigation service.On the categories of data processedL Article 2 of the draft decree lists the personal data and information that can be processed, distinguishing between those relating to the declarant, the agent processing the report, and the facts reported. Article 3 also provides that the processing may record sensitive data within the meaning of article 6 of the law of January 6, 1978 as amended. Firstly, the Commission observes that the declarant is not obliged to provide all the data referred to in Article 2 and that he will be able to connect to the platform without providing data allowing him to be directly identified. . To this end, article 2 includes in the data that can be collected pseudonyms, aliases and nicknames, which was not previously provided for. By allowing the use of pseudonyms, the new device promotes the use of the platform and facilitates exchanges. The collection of the IP address and the source port attached to the declarant, which will be carried out automatically when connecting to the platform, is on the other hand likely to attenuate the possibility of using the PNAV in a pseudonymised way. In this respect, the Commission takes note of the

clarifications provided by the Ministry according to which these data will only be used in certain circumstances, for example in the event of an emergency requiring the protection of a person who has not been identified or malicious service. It observes that the use cases envisaged correspond to those selected for the platform for reporting sexual and gender-based violence, on which it has already ruled in its deliberation n°2018-310 of September 13, 2018. In any case of cause, the ministry should delimit the cases of exploitation of the IP address and the source port in a doctrine of use and, moreover, envisage a training of the personnel in this direction to avoid any treatment which would not be necessary in previously identified situations. The Commission takes note of the fact that an employment doctrine is currently being drawn up, and of the Ministry's commitment to communicate it to it. Secondly, the Commission notes that the processing may record sensitive data, exception of genetic and biometric data. In accordance with article 88 of the law of January 6, 1978 as amended, the processing of such data is only possible in the event of "absolute necessity, subject to the appropriate guarantees for the rights and freedoms of the person concerned". With regard to the necessity of the processing, the Commission observes that the collection of the sensitive data covered by the draft decree cannot be excluded with regard to the architecture, the purposes and the scope of the offense covered by the PNAV. Indeed, the data likely to be collected are intended to be entered by the declarant using the free field of instant messaging. They can therefore concern both declarants and third parties and concern offenses involving personal injury. However, the exchanges relating to some of these offences, such as discrimination, involve the communication of sensitive data by the declarants. In this regard, the ministry specified that it is not possible to exclude that sensitive data is communicated by the declarant and that, moreover, the establishment of a filter device would lead to restricting the operator in the exercise of its missions and the user in his declaration. With regard to the guarantees surrounding the processing of this sensitive data, the Commission takes note of the clarifications provided by the Ministry according to which the only data necessary for the purpose of the processing and corresponding to the facts reported will be retained by the operators. This minimization will be guaranteed in particular by the training, specialization and supervision of operators on the one hand, and by the development of an employment doctrine explaining the data that can be collected on the other hand. In addition, the Commission observes that it will not be possible to carry out a search within the platform using sensitive data, which moreover cannot be subject to extraction, in particular for the purposes of compiling statistics. thirdly, the Commission observes that any exchange carried out on the web platform will be subject to the prior collection of the declarant's postcode or municipality of residence. These data, whose collection has the sole purpose of directing the declarant to the territorially competent services,

will nevertheless be kept in the processing. The Commission wonders whether it is necessary to record this data once the declarant has been directed to the competent department and that, as a result, the purpose of the collection has been achieved. Subject to the comments made above, the Commission considers that the categories of data covered by the draft decree are adequate, relevant and not excessive with regard to the purposes for which they are collected. On the retention period of data Article 4 of the draft decree provides that personal data and information referred to in the aforementioned Article 2 are kept for the time strictly necessary for reporting, for a period not exceeding four hours from the last exchange. Firstly, the Commission notes that the "last exchange" corresponds to the last message appearing in the current discussion thread and that, moreover, a user leaving the platform and subsequently reconnecting with an address e IP and an identical source port would see a new exchange open. Secondly, the data and information collected will be automatically deleted after the maximum period provided for by the draft decree. They may, moreover, be subject to manual deletion by the operator at the end of a conversation and even before the expiry of the four-hour period. In this regard, the Commission stresses that the manual deletion of data at the end of a conversation should be the subject of a specific point of awareness among operators, so that any data not necessary for the purposes of the processing be withdrawn as soon as possible. On the connections envisaged The Commission notes that the Ministry plans to connect PNAV with N-MCI and LRPGN processing, and that these connections aim to ensure the processing of the reports made by the declarants on the platform. As a preliminary point, it observes that the data constituting a report entered on the PNAV may be entered into one of the aforementioned processing operations with a view to establishing an account. report report. This data will only be recorded in N-MCI or LRPGN if the facts reported by the declarant are consistent with the purposes of the processing and are linked to one of the offenses falling within the categories referred to in Article 1 of the draft decree. Finally, the transmission of data from the PNAV to one of the aforementioned processing operations will lead to the closure of the conversation on the platform and, thereby, to the deletion of the latter. N-MCI will be transitional, insofar as the ministry intends to create a new process allowing the collection of reports from individuals in the police station, which will be intended to be linked to the digital platform for supporting victims. temporary, the linking of PNAV and N-MCI treatments raises observations. In this respect, the Commission recalls that the linking of processing operations governed by regulatory acts must comply with the provisions governing each of the processing operations, in particular with regard to the purposes, categories of data, users and recipients of the two processing operations. In this case, the proposed connection is not contrary to the purposes of the two processing operations in that it aims to

transmit, to the competent investigating services, reports requiring judicial processing. However, some of the categories of data that may be collected under the PNAV and therefore likely to be paid in the N-MCI treatments are not authorized to be included in the latter. In particular, the processing of sensitive data is not authorized by the decree of June 22, 2011 governing N-MCI processing. The Commission recalls having underlined, in its deliberation n°2011-125 of May 5, 2011, that the wording and legal form of the text governing N-MCI do not allow the processing of sensitive data. Under these conditions, the Commission invites the Ministry to make only the connections that would be relevant with regard to the purposes of the PNAV and compatible with the provisions governing each of the processing operations. On users and recipients of processing Article 5 of the draft decree relating to users and recipients of processing essentially repeats what exists for the platform for reporting sexual and gender-based violence. It nevertheless provides details on certain categories of people who can access personal data and information recorded in the processing. Thus, the psychologists of the national police and gendarmerie assisting the personnel responsible for collecting reports may, under victim support system, receive all personal data and information referred to in Article 2, except for the IP address and the source port. The Commission notes that other categories of data listed by article 2, such as the e-mail address of the declarant, are not necessary for the accompaniment of the victims. In addition, the transmission of this data may be carried out by telephone, a means of communication likely to promote the spontaneity of exchanges and therefore the transmission of data not necessary for the support of a victim. In the light of these elements, the Commission invites the Ministry to take appropriate measures to ensure that the operators of the platform communicate to the psychologists of the national police and gendarmerie only the relevant and necessary data to support a victim.Finally, the Commission underlines that the transmission of data by means of a means of communication by telephone is also likely to raise issues relating to the security of the processing, which should be taken into account where appropriate.On the procedures for exercising rights As a preliminary point, the Commission observes that the procedures for exercising rights are similar to those of the platform for reporting sexual and gender-based violence. On the one hand, the rights to information, access, rectification and erasure and to the limitation of data will be exercised directly with the general management of the national police and the general management of the national gendarmerie. On the other hand, the rights of access, rectification, deletion and limitation may be subject to restrictions under the conditions of 2° and 3° of II and III of article 107 of the law. of 6 January 1978 as amended. Finally, the right of opposition will not apply to processing pursuant to article 110 of the law of 6 January 1978 as amended. Firstly, the Commission notes that general information will be provided to the public via a

confidentiality policy, accessible on each page of the "service-public.fr" site hosting a communication channel, which will specify the scope of application and scope of processing. Processing information will also be provided on the ministry's website. The Commission observes that, given the very purpose of the processing, the persons mentioned by the declarant as author, victim or witness will not have information on the fact that they are, where applicable, the subject of a report, neither on the declarant who mentions them, nor on the facts likely to be imputed to them, nor on the conservation of these elements for a period of four hours. Secondly, the exercise of the rights of access, rectification, erasure and limitation of the persons mentioned as authors, victims or witnesses by a declarant will also be limited insofar as these persons have not not intended to be aware of the report in question. In this regard, the Commission observes that the persons concerned will be more numerous than under the previous system, in particular with regard to the extended scope of the platform, which aims to cover a wide range offenses of harm to persons on the one hand, and is accessible to people who believe they are victims or witnesses of one of these offenses on the other hand. In order to limit the number of people whose data are processed and whose the exercise of rights is limited in practice, the Commission invites the Ministry to take into account the principle of data minimization. In this sense, it reiterates the need to make operators aware of the collection of only personal data and information strictly necessary for the purposes of the processing and relevant in a given exchange. On the planned security measures Firstly, access to the teleservice will be done via the HTTPS protocol, which guarantees the confidentiality of the data exchanged as well as the authentication of the data controller. Regarding the use of this protocol, the Commission recommends using the most up-to-date version of TLS possible. In particular, it recalls that the TLS 1.0 and TLS 1.1 versions do not have RGS-compliant cryptographic functions. In addition, the Commission recommends the implementation of all ANSSI's recommendations on the subject, formalized in the document "Security recommendations relating to TLS" which was updated in March 2020 by a version 1.2. Finally, it recalls that it is up to the ministry to formally certify the acceptance of the security level of the teleservice through a general security reference standard (RGS) approval as provided for by decree n ° 2010-112 of February 2 2010 and to publish the certificate of approval on its site.Secondly, the Commission notes that the storage of open files will be carried out at a host guaranteeing hosting on a platform not subject to extra-European legislation . Concerning the EASICHAT instant conversation subsystem, the Commission recalls that the data processed by this subsystem must be hosted under the same conditions as those of the open files, or failing that, additional encryption measures are implemented in order to guarantee the technical impossibility for the host to access the data in plain text. deliberation

n°2017-190 of June 22, 2017. It underlines, in particular, the importance of using a non-reversible and secure cryptographic function specialized in the storage of passwords. Fourthly, it appears that logging of creation, modification, consultation, communication, transfer and deletion of data will be implemented. All traces will be kept for three years. The Commission takes note of this duration with regard to the stored files. For the traces relating to the exchanges, themselves integrated into the business software if necessary and deleted after four hours of PNAV processing, it considers that a shorter duration should have been adopted. In any event, and in order to limit the risks of non-detection of abnormal use of the device, the Commission recommends carrying out an automatic control of the traces, generating alerts if necessary, as well as a regular review authorizations and checks on their use. Finally, the Commission notes that the Ministry has implemented several measures aimed at limiting the risks of discovery of the use of the platform by third parties, such as a red button "Leave urgently and delete the conversation", an insignificant choice of URL or information on the deletion of traces made available to victims on the main site directing victims to the PNAV. Subject to the above observations, the Commission considers that the security measures described by the data controller comply with the security requirements provided for by article 99 of the law of January 6, 1978 as amended. However, this obligation requires the updating of security measures in the light of the regular reassessment of the risks. In this respect, the Commission stresses that specific attention should be paid to the reassessment of security measures the imperative update of the impact assessment.The PresidentMarie-Laure DENIS