

Deliberation 2021-059 of May 20, 2021 Commission Nationale de l'Informatique et des Libertés Nature of the deliberation: Opinion Legal status: In force Date of publication on Légifrance: Friday March 18, 2022 NOR: CNIX2200795V Deliberation n° 2021-059 of May 20, 2021 providing an opinion on a draft decree creating an automated processing of personal data called the "Interministerial PPST Base" (request for opinion no. 20016935) The National Commission for Computing and Freedoms, Seized by the General Secretariat for Defense and national security of a request for an opinion on a draft decree creating an automated processing of personal data called "Interministerial PPST database"; Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 31-II; After hearing the report of Mr. François PELLEGRINI, commissioner, and the observations of Mr. Benjamin TOUZANNE, government commissioner, Issues the following opinion: The Commission has been seized by the General Secretariat for Defense and National Security (SGDSN) of a request for an opinion concerning a draft decree (hereinafter "the draft decree") creating an automated processing of personal data called "Interministerial PPST database" (hereinafter "interministerial database "). This processing aims to contribute to the system for protecting the scientific and technical potential of the Nation (PPST), which is based on controlling access to strategic or sensitive knowledge, know-how and technologies housed in restricted regime zones (ZRR), in such a way as to prevent the risks of capturing or misappropriating them. ministerial bases"), which allow the ministers concerned to examine the requests for advice referred to them, pursuant to Article R. 413-5-1 of the Criminal Code, by the heads of departments, establishments or companies called upon to rule on a request for authorization to access a restricted regime zone (ZRR). He must also centralize the personal data and information recorded in the processing called "SOPHIA" which notably allows the Ministry of the Armed Forces to manage access to the ZRRs under its supervision. This processing must thus provide overall visibility on the access authorization requests that have been recorded and thus determine whether other access requests submitted by the same person have already been processed by other ministries as well as, if where appropriate, the follow-up that has been given. In general, the Commission recalls that particular vigilance is required with regard to this type of system, the purpose of which is in particular to carry out administrative security investigations. Given the fact that this processing aims, on the one hand, to protect knowledge, know-how and technologies relating to national defense or the fundamental interests of the Nation and, on the other hand, to prevent their misappropriation for military purposes, terrorism or of proliferation of weapons of mass destruction, the Commission considers that it falls under Articles 1 to 41 of the amended law of 6 January 1978 as well as Articles 115 to 124 of the same law applicable to internal processing. security of the

State and defence. On the purposes of processing Article 1 of the draft decree specifies that the purpose of processing is to prevent essential elements of the scientific or technical potential of the Nation, on the one hand, from being the object of capture likely to weaken the means of defense of the Nation, to compromise its security or to harm its other fundamental interests and, on the other hand, to prevent their diversion for the purposes of terrorism, proliferation of weapons of mass destruction and their vectors, or contribution to the increase of military arsenals. The purpose of the processing is the integration of personal data and information recorded in the ministerial bases and in the processing called "SOPHIA" . In doing so, it must provide visibility of all access authorization requests that have been recorded. The interdepartmental database thus aims to promote exchanges between the departments and allow cross-checking of information, if necessary (for example, the identification of discrepancies in access request files submitted by the same person to different departments). Without calling into question the need for the services of senior defense and security officials (HFDS), responsible for examining requests for advice, to verify whether the persons at the origin of the requests for access to a ZRR have carried out other requests to other ministries, and to know the consequences thereof, the Commission considers that the wording of Article 1 of the draft decree, according to which the processing "aims to enable the recipients of this processing to have visibility on all access authorization requests that have been recorded", is too broad. It notes that the SGDSN plans to replace these terms with the following wording: "the purpose of which is to verify, for the purpose of examining requests for advice, whether a person requesting access to a restricted area has already presented one or more requests to other ministries, and, if necessary, to allow them to know the follow-up which has been given to them". Subject to this reservation, the Commission considers that the purposes of the processing are determined, explicit and legitimate. On the data collected Article 2 of the draft decree specifies that the personal data and information recorded in the interministerial database come from ministerial databases, which centralize the instruction by the ministries concerned of requests for advice relating to requests for authorization to access a ZRR. The Commission also notes that the inter-ministerial database will also be fed with personal data and information resulting from the processing called "SOPHIA" implemented by the Ministry of the Armed Forces. The Commission takes note of the information provided by the SGDSN according to which the implementation in relation between the ministerial bases and the inter-ministerial base will operate only from the first to the second, in order to import into the latter, via an exchange file transported manually from one base to another, the data from the bases ministerial. This operation will be carried out at regular intervals (at least once a week), on the initiative of the ministries concerned. This feeding of the interministerial database by

the ministerial databases is justified by the fact that the processing of requests, in each ministerial department, requires checking, on the one hand, whether the same person has made requests in other ministries and , on the other hand, if this is the case, to consult certain parts of these other requests in order to identify malicious applicants. The purpose sought by the government can be achieved either by the total duplication of the ministerial bases in the interministerial base, by the transmission of only relevant files, when the need arises during an investigation. The Commission recalls that its doctrine, based both on the principle of data minimization and data security, strongly advises against the duplication of databases when they contain sensitive information, which is the case in 'species. The Commission does not dispute that it is necessary for all the names and identification information of the applicants present in the ministerial databases to be copied into the interministerial database so that the interrogation of the latter, by the persons authorized in each ministry, makes it possible to determine whether it is necessary to access the additional elements stored in the ministerial databases. On the other hand, the advance transmission of all the personal data and information recorded in the ministerial databases appears to go beyond what is necessary, since it is only occasionally that some of this information will have to be consulted in the interdepartmental database. If the bases could have been linked together by network APIs, the Commission would have recommended that the funds of the files to be consulted be uploaded on demand to the interdepartmental database, according to needs. The special procedures for exchanging information between the ministerial bases and the ministerial base, via a removable medium rather than by network interconnection for reasons of partitioning, are not such as to call into question this principle, the exchange of information between databases being always provided by the support shuttle. Consequently, given the nature of the data in question, the fact that the checks to be carried out concern, according to the elements brought to its attention, only a limited number of files in relation to all the data from each ministerial database which would be duplicated, and to the fact that it is not justified that another use of the interministerial database by its accessors would require permanent access to the all of these data, the Commission considers that this solution should be favoured. It therefore invites the SGDSN to ensure that the interministerial database allows the investigating officers who can access it to check whether the name of the applicant in question is present in other ministerial databases and, when this is the case, that the system of the interdepartmental database generates a transfer request for the relevant elements from the ministerial databases to the interdepartmental database, similar to what would be done using a network API. These requests would be automatically transmitted, and their results automatically repatriated, during the support shuttle. According to the information available to the Commission, the

interministerial database is updated every week, and the resulting extension of the investigation times would be limited. It invites the government to provide secure methods for timely feeding of the interministerial database in order, in particular, to protect the identity of the people whose data is transferred to this database, and to delete data that has become unnecessary within the interministerial database. once the checks have been carried out. The Commission also wonders whether it is necessary to include, under the category "information contained in the documents provided to the head of the department, establishment or company by the person the subject of the request for an opinion", all the information, documents and documents provided by the applicant as part of his access request file (curriculum vitae, letters of recommendation, list of publications, studies or works made, copies of diplomas or identity documents, etc.). On the retention period of data Article 4 of the draft decree provides that personal data and information recorded in the processing are kept for a period of ten years and two months from the date of transmission of the last opinion issued by the Minister on a request for access to a ZRR. The Commission takes note of the information provided by the SGDSN according to which this duration is justified, on the one hand, by the fact that an authorization to access a ZRR is granted for a maximum period of five years and, secondly, by the Minister's interest in knowing whether the author of the request for access has already submitted a request for access to a ZRR and, if so, to take note of the elements of the instruction which had then led to issuing a favorable opinion or not. In view of these elements, the Commission considers that such a retention period is proportionate. It recalls that the purpose of the processing in Article 1 of the draft decree must be specified in order to indicate that the interministerial basis aims to enable the ministries concerned to examine the requests for advice for which they are responsible. The Commission considers finally that the implementation of a system for uploading into the interministerial database, by means of a manually transported exchange file, the relevant elements of the ministerial databases, following the request of the investigating officers, entails that the data personal data and corresponding information be deleted from the inter-ministerial database once the Minister's opinion has been given. On the accessors and recipients of data Article 5 of the draft decree lists the persons who can access personal data and information recorded in the treatment as well as the recipients. First, the recipients of personal data and processing information, the agents of the six ministries mentioned above and responsible for examining requests for advice, individually designated by the minister responsible for them and specially authorized by the SGDSN. agents are the people who, within the ministries, are in charge of the implementation of the PPST system (the PPST project managers and their direct hierarchy). These agents are authorised, because of their function which involves processing requests for advice, to

access, for the sole purpose of their consultation, all the data and information recorded in the interministerial database.

Secondly, article 5 of the draft decree provides that the agents of the specialized services mentioned in the first paragraph of article R. 811-1 of the internal security code, known as "first circle intelligence services", individually designated by the supervisory authority to which they report and specially authorized by the SGDSN, may be recipients of the information recorded in the processing. directly associated with the implementation of the PPST system through the prevention, information and inspection missions for which they are responsible. It therefore considers that the communication of information to these services is part of the purpose of protecting the essential elements of the scientific or technical potential of the Nation provided for in Article 1 of the draft decree. In this respect, the SGDSN specified that the agents concerned are in particular those coming under the Directorate of Intelligence and Defense Security (DRSD) and the General Directorate of Internal Security (DGSI). The Commission therefore considers that the draft decree should be modified in order to target only these two specialized intelligence services and notes that the SGDSN plans to modify Article 5 of the draft decree accordingly.

Article 7 of the draft decree provides that the ministerial bases as well as the automated processing of personal data relating to the management of the security procedures of the personnel of the Ministry of Defense and Industries, referred to as "SOPHIA", are the object of a link with the interministerial database. In this respect, the SGDSN specified that these links will operate from the ministerial databases and from the processing called "SOPHIA" to the interministerial database, via a file of exchange. This operation will be carried out at regular intervals (at least once a week), on the initiative of the ministries concerned. , the Commission notes that the purposes it pursues are significantly broader and concern, under the terms of Article 1 of the decree of 30 April 2014 establishing the processing, on the one hand, the dematerialized management of the procedures of security clearance and elementary control carried out within the framework of the protection of national defense secrets and, on the other hand, the management of permission requests from soldiers abroad within the framework of the protection of defense personnel. Article 7 of the draft decree provides that the connection between the inter-ministerial database and the "SOPHIA" processing is carried out "within the framework of the purpose defined in Article 1 and within the limits of the necessary information". In this regard, the Commission considers that this import of personal data and information should be limited to data relating to requests for access to ZRRs. It notes that the SGDSN plans to modify article 2 of the draft decree in order to specify that the personal data and information resulting from the "SOPHIA" processing recorded in the interministerial database will only concern requests for access to the ZRR .Finally, it considers that the decree of April 30, 2014

establishing the processing should be amended in order to provide for the envisaged connection. On the rights of individuals Article 8 of the draft decree provides that the right to information provided for in I article 116 of the amended law of 6 January 1978 does not apply to the processing. In this respect, the SGDSN considers that, insofar as it does not directly collect personal data and information concerning the person making the the subject of the request for an opinion, he may be exempted from the obligation to inform the person concerned, who will have been informed in advance by the head of the department, establishment or company when the fo Access authorization request form. The Commission notes that the information appearing on the access request forms completed by persons when they submit a request for access to a ZRR, will specify that the data of a personal nature and the information collected is subject to an automated processing of personal data called "Ministerial PPST database" and another called "Interministerial PPST database". It also stresses that the publication of the regulatory act governing the processing is part of informing the persons concerned with regard to the processing of their personal data. The Commission therefore considers that information is not impossible and that it is even planned and asks the SGDSN to modify article 8 of the draft decree in this direction. It notes that the indication that the right to information does not apply will be deleted and that the article 8 of the draft decree will specify that information in accordance with the provisions of I of article 116 of the amended law of 6 January 1978 appears on the ZRR access request form. The other provisions of the draft decree relating to the absence of the right to object and the right of access being exercised indirectly do not call for any comments from the Commission. On data security The Commission considers the security measures that will be implemented to be satisfactory. The President Marie-Laure DENIS