

Deliberation 2021-001 of January 7, 2021 Commission Nationale de l'Informatique et des Libertés Nature of the deliberation: Opinion Legal status: In force Date of publication on Légifrance: Friday February 19, 2021 NOR: CNIX2103055V Deliberation n° 2021-001 of January 7, 2021 providing an opinion on a draft decree creating an automated processing of personal data called "FL@sh EVENT" relating to the reporting of serious events (request for opinion no. 20020614) The National Commission for Computing and Liberties, Saisie by the Minister of the Armed Forces of a request for an opinion concerning a draft decree creating an automated processing of personal data called FL@sh EVENT relating to the reporting of serious events; 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 (GDPR); Having regard to the Defense Code, in particular its Articles R.* 1142-1 and R.* 3111-1 et seq.; Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 6-III; Considering the decree n° 2019-536 of May 29, 2019 taken for the application of the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms; After having heard Mr. Alexandre LINDEN, commissioner, in his report, and Mr. Benjamin TOUZANNE government commissioner, in his observations, Issues the following opinion: The National Commission for Computing and Liberties (hereinafter the Commission) was seized by the Minister for the Armed Forces with a request for an opinion relating to a draft decree in Council of State creating an automated processing of personal data called FL@sh EVENT relating to the reporting of serious events which have been set by a ministerial instruction. This processing must make it possible to bring to the attention of several departments of the Ministry of the Armed Forces and, where appropriate, of the Minister, any serious event involving, as victim or perpetrator, military personnel or civil law in a case likely to have disciplinary, criminal or media consequences. The Commission thus immediately notes the particularly wide scope of the system envisaged, which must therefore be subject to strictly defined conditions of implementation and be surrounded by satisfactory guarantees. The Commission notes that the FL@sh EVENT processing is put implemented solely for the purposes of informing the Minister, staff, directorates and departments of the Ministry of the occurrence of these events (tool aimed at ensuring the feedback of information) and is not intended to organize the investigation of any disciplinary or legal follow-up given to these events and carried out through other processing. In this regard, it notes that several guarantees are provided, including the absence of connection with other processing of personal data. Given the purposes pursued by the FL@sh

EVENT processing as well as the clarifications provided by the Ministry, the Commission considers that the provisions of the GDPR should be applied. It also notes that the Ministry intends to rely on the legal basis for the performance of a mission of public interest, in accordance with Article 6.1.e of the GDPR. Insofar as data mentioned in I of article 6 of law n° 78-17 of January 6, 1978 as amended above (sensitive data excluding genetic and biometric data) are likely to be recorded in the processing FL@sh EVENT, the ministry considers that its creation must be the subject of a decree in Council of State taken after reasoned and published opinion of the Commission, in accordance with article 6-III of this same law. The Commission notes that as it stands, the decree provides not only for the transmission of event reports, but also for the constitution of a file systematically storing these reports for a period of five years. On the operation of the FL@sh EVENT processing and the purposes pursued Article 1 of the draft decree specifies that the sole purpose of the processing is to bring to the attention of the staffs, directorates and departments of the ministry and, if necessary, of the Minister of Defence, the occurrence of serious events. This same article specifies that the serious events likely to be the subject of a report are those involving, as victim or perpetrator, military or civilian personnel in a case likely to have disciplinary, criminal or media consequences. or causing serious harm to the domain and property of the Minister or of the public establishments that depend on it. The Commission thus notes that the processing implemented concerns events occurring within the Ministry of the Armed Forces or the public establishments that depend on it, as well as all those who could be associated with this ministry without directly involving it. It thus takes note of what are likely to be concerned with events whose perpetrator or victim is a member of foreign military forces in transit on national territory or a civilian in the context of an event that took place in a military control (such as a drone overflight). The Commission takes note of the clarifications provided by the Ministry according to which the processing constitutes a procedure for immediate reporting and simple information to the aforementioned high authorities for communication purposes (up to crisis communication) and thus aims to replace the authority messaging systems used within the Ministry of the Armed Forces. However, it notes that such a clarification does not appear in the draft decree and considers that Article 1 should be amended in order to explain the purpose pursued by the feedback of information operated through the FL@sh EVENT processing. Such clarification would help to remove any ambiguity, particularly with regard to the use of the information contained in this processing for the purposes of possible prosecution (disciplinary and legal). The Commission notes that the FL@sh EVENT processing is based, from an operational point of view, on the drafting of a report form, including a brief summary of the facts as well as the measures taken or envisaged in this respect, by the head of organization or a

person designated by him for this purpose (the editor). This writer thus analyzes the sensitivity of his report after having examined the circumstances and the supposed consequences of the event. If he considers that the event is particularly serious and must be brought directly to the attention of the office of the Minister for the Armed Forces, he chooses the FL@sh MIN format. If, on the other hand, he considers that the event is less serious for the institution, he chooses the FL@sh ADS format which is then transmitted to a chain of recipients according to the ADS concerned (for the army, general management, direction or service of the ministry). Finally, the Commission notes that the initial report may be updated in order to make corrections or additions to an imprecise or inaccurate report and that this update will be carried out in an apparent manner. The Commission notes that it results from the operation even of the FL@sh EVENT processing that any fact related to the activity of the Ministry of the Armed Forces is likely to constitute a serious event likely to appear in this processing with the exception, however, of certain categories of events specified by a ministerial instruction of April 30, 2020 (No. 20/ARM/CAB/CM11/NP), subject to specific reporting procedures, such as nuclear events. While the Commission notes that the events that may give rise to a report in FL@sh EVENT processing have been listed in the context of the aforementioned ministerial instruction of 30 April 2020, it notes that some of them seem particularly broad or are not the subject of a sufficient degree of detail to enable their seriousness to be assessed. This is the case, for example, of the Other events - Personnel category, which allows information to be entered on any other serious event related to personnel. The Commission deduces from the foregoing that in practice, any fact which, in the opinion of the authority concerned, is of particular importance from the point of view of its nature, its circumstances, the persons involved or its possible consequences is likely to be the subject of information feedback via FL@sh EVENT processing, including when no personal data is provided. In the absence of a criterion making it possible to qualify a threshold of seriousness with regard to the events brought to appear in this processing, it recalls the importance of strictly understanding this notion of seriousness. In view of the foregoing, the Commission considers that Article 1 of the draft decree should be amended in order to cover only events considered serious within the meaning of the aforementioned ministerial instruction. Finally, the Commission notes that, according to the Ministry, the criteria likely to make the performance of a data protection impact assessment (DPIA) mandatory are not met. It observes, however, that the FL@sh EVENT processing is in particular likely to contain sensitive data and that it is not possible to exclude, with regard to the particular nature of the processing, that the persons concerned, when they are members Ministry personnel, are considered as so-called vulnerable persons, with regard to the relationship of subordination resulting from the employment relationship. Under these

conditions, the Commission considers that a DPIA should be carried out and sent to it only in the event that it reveals high residual risks. On the data collected Article 2 of the draft decree provides that data relating to the identity of the persons involved in the occurrence of a serious event, their professional life as well as those relating to the description of the serious event, the circumstances in which it occurred and the follow-up given to it, excluding any data relating to criminal convictions .

The Commission notes that the following data may be collected under the category relating to the identity of persons: - the status of the person: presumed perpetrator, presumed victim or presumed witness; - the category of personnel: officer , non-commissioned officer/petty officer, non-commissioned member, personnel of category A, B or C; - the army, direction or service employing the person; - the army, direction or service managing the person; - the gender of the person; - the rank, surname, first name and defense identification number of the person. In view of these elements, the Commission requests that article 2 of the draft decree be clarified in this sense. data collected in respect of professional life, the Commission notes that the category of military or civilian personnel will be recorded as well as the reference to the army, management or service manager or employer. The Commission also notes that the data recorded under this category in the FL@sh EVENT processing is likely to overlap with some of the data recorded under the identity category of persons (such as the category of staff or grade, etc. .). Although it notes that the ministry has undertaken to provide an appendix to the decree detailing the data collected, it considers that it would have been preferable to include them directly in the decree. It recalls, in any case, that only the data strictly necessary for the purpose pursued by the processing should be collected under this category. The Commission also notes that the writer of the report describes the serious event as well as the circumstances in which it occurred, the action taken, excluding any data relating to criminal convictions by filling in the free fields. The Commission recalls, in general, that the data processed must be relevant, adequate and not excessive with regard to the purpose pursued and that it is up to the ministry to ensure strict control of the data entered via these free fields. It considers this control all the more essential as sensitive data may be collected depending on the nature of the event reported in FL@sh EVENT. In this respect, while the Commission takes note of the fact that there is a framework to encourage the writer to provide only the information necessary for the proper functioning of the system, it nevertheless invites the ministry to introduce a system making it possible to filter the terms which will have previously been defined as prohibited in order to ensure the relevance of the information collected and its non-excessive nature. The Commission also notes that data relating to the offenses mentioned in Article 10 of the GDPR could nevertheless be processed. In this respect, it notes that the Ministry intends to avail

itself of the provisions of Article 46-1° of Law No. 78-17 of 6 January 1978 as amended and draws its attention to the need to record only the data strictly necessary to the purpose pursued by the processing. Finally, the Commission notes that while documents may be attached to the report (description of the event by the protagonists, report of the filing of a complaint, etc.), no copy of any document identity, photograph or video recording is collected. On the retention period Article 3 of the draft decree provides that personal data and information recorded in the processing are kept for a period of five years from the date of their recording. This data may be kept beyond this period in the event of litigation before an administrative or criminal court, until the dispute has been finally ruled on or until the judicial inquiry is closed. The Commission notes that these retention periods have been decided in collaboration with the Defense Historical Service as part of an archiving strategy. According to the Ministry, this period of five years corresponds to the usual period for the retention of personal data, in particular for the purposes of initiating disciplinary proceedings and managing legal remedies. While the Commission takes note of these clarifications, it recalls that under the terms of Article 5 of the GDPR, personal data must be kept for a period not exceeding that necessary for the purposes for which they are processed. Insofar as the FL@sh EVENT processing only pursues a purpose of information within the framework of the occurrence of serious events and not of instruction of the disciplinary or judicial follow-up given to these events, the Commission wonders about the reasons which led to keeping, in principle, the reports for five years and not for the duration strictly necessary for the feedback of information. With regard to the purposes pursued by the FL@sh EVENT processing, it considers that such a retention period for this data, on an active basis, does not appear proportionate. While it notes that discussions are currently underway to consider the creation of an intermediate archiving database, it notes that no other information has been sent to it. On accessors and recipients Article 4 of the draft decree details the list of accessors and recipients of FL@sh EVENT processing and provides for three distinct levels of access to information: persons who can access, for the sole purpose of consultation, information strictly necessary for their mission; the persons who can access, for the purposes of consultation and modification, the information strictly necessary for their mission; the persons who can access, for the purposes of consultation and modification, all the information. In general, the Commission draws the Ministry's attention to the need to manage with the greatest vigilance the authorizations of the personnel concerned, in order to limit to what is strictly necessary the persons likely to access information or receive communication from it. In this respect that the data relating to acts of prosecution and to security measures taken by a judge are subject to stricter rules. Communication rules and are only accessible to certain categories of people. The Commission also

notes that the list of organizations automatically receiving information and personal data according to the category of FL@sh MIN or FL@sh ADS events is specified by the aforementioned ministerial instruction of 30 April 2020 . The Commission notes that according to this instruction, it is a question of allowing the transmission of data according to the categories of events outside hierarchical chains. In order to clarify the system as a whole, it requests that article 4-III of the draft decree be clarified in this sense. The Commission also observes that certain categories of recipients automatically receive communication of information according to various criteria, namely the category of event, the issuer's chain of command, the nature of the report, or even according to information given by the issuer in the report (operational chain, geographical area, etc.). The signatory can also add additional recipients that he or she considers relevant. In this respect, the Commission draws the Ministry's attention to the need to ensure that, in accordance with the principle of respecting the need to know, only persons for whom the information is strictly necessary for their mission actually have it. knowledge. The Commission also notes that the Defense Intelligence and Security Directorate (DRSD) systematically receives alerts transmitted via FL@sh EVENT. If this transmission is justified by the missions entrusted to the DRSD by virtue of articles D. 3126-5 and following of the Defense Code, it recalls that this transmission for information purposes only must not lead to the data from of FL@sh EVENT are linked, in any way, with the processing implemented by the DRSD. On the other conditions for implementing FL@sh EVENT processing On the rights of individualsThe Commission notes that general information will be published and that the person making the report may also be provided with specific information via their connection to the application. It takes note of the clarifications made according to which individual information could compromise the very purpose of the processing. The Commission notes that if Article 6 of the draft decree provides that the rights of access, rectification, limitation and opposition provided for in Articles 15 et seq. of the GDPR apply, the right to erasure is as far as excluded him. If it considers, with regard to the purposes pursued by the FL@sh EVENT processing, that this exclusion is not likely to excessively infringe the rights and freedoms of the persons concerned, the Commission wonders about the reasons which led to maintaining , at the same time, the right to object, the exercise of which, in view of the functionalities of the processing, seems difficult to carry out. On security measures and transfers outside the European Union (EU) The Commission takes note of the clarifications provided according to which functional identifiers will be used to manage access to processing, which seems to suggest that certain accounts will thus be shared between different users. It recalls that the accounts allowing access to the processing of personal data must be nominative and that the identifiers and passwords must be individual, defined by the users and known only to them, and takes

note of the commitments of the ministry in this sense. The Commission notes that Article 5 of the draft decree provides for the retention of traces for a period of one year from their recording. This same article also provides that each operation is the subject of a recording including the identification of the user, the date, the time and the nature of the intervention. The Commission recalls that the main purpose of the processing of supervision logs is to detect and prevent illegitimate operations on the main data. In this context, the Commission specifies that automatic or semi-automatic proactive trace analysis mechanisms, as well as organizational measures, must be implemented in order to identify most illegal behavior. The Commission therefore considers that a retention period for the logs of six months is sufficient to use this information. The Commission also takes note of the information provided by the Ministry according to which: accessible only from the ministry's internal network, regularly approved and considered to be safe; - the software used is commonly used software, the source code of which is publicly available, which provides a significant guarantee as to its reliability. The Commission takes act that no transfer of data to a State outside the European Economic Area or to a recipient established in a State not belonging to the EU is carried out. It recalls that data transfers to third countries can only be carried out subject to compliance with the conditions set out in Articles 45 and following of the GDPR. In the absence of an adequacy decision adopted by the European Commission, such transfers will not can be made only subject to appropriate safeguards being implemented in accordance with Article 46 of the GDPR, taking into account the circumstances of the transfer as well as the recommendations of the European Data Protection Board on the measures which complement the tools of transfer to guarantee compliance with the level of protection of personal data of the EU. The President Marie-Laure DENIS