Deliberation 2022-110 of November 10, 2022Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Saturday February 11, 2023NOR: CNIX2303383XDeliberation n° 2022-110 of November 10, 2022 providing an opinion on a draft decree authorizing the implementation of automated trace management processing relating to the information and communication systems of the Ministry of Defense (request for opinion no. 21011213) NOR: The National Commission for Information Technology and Freedoms,Seizure by the Ministry of the Armed Forces of a request for an opinion concerning a draft decree authorizing the implementation of automated processing for the management of traces relating to the information and communication systems of the Ministry of Defence, Considering the modified law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms, and in particular its title IV; After having heard the report of Mrs Isabelle LATOURNARIE-WILLEMS, auditor, and the observations of Mr .Benjamin TOUZANNE, Government Commissioner,Being reminded of the following elements:The Commission has been seized of an order which aims to regulate the implementation of automated processing for the management of traces relating to information and communication systems in the States - majors, directorates and departments of the Ministry of the Armed Forces. This text constitutes a single regulatory act within the meaning of IV of article 31 of the aforementioned law of January 6, 1978. It is therefore intended to regulate processing that serves the same purpose, relates to identical categories of data and has the same recipients or categories of recipients. communication of the Ministry of Defense referred to in Article 1 of Decree No. 2018-532 of June 28, 2018 establishing the organization of the defense information and communication system and creating the General Directorate of digital and information and communication systems. With regard to their purposes, these processing operations are intended to be governed by Title IV of the law of January 6, 1978. the threat of cyber origin and is based on the need to be able to identify irregularities in access to or use of information systems. In this respect, the Commission recalls that the traceability of actions is an elementary measure of the security of processing and that the proactive analysis of traces is an essential measure for the effective use of traceability. The project to deploy trace management processing within the Ministry of the Armed Forces is part of this perspective, and thus responds to the Commission's recommendations regarding the need to develop logging tools. planned devices will be perimeter logging systems, which are therefore not intended to ensure the operational traceability of business processing, but to contribute to the overall implementation of security. It recalls in this respect that, for business processing that will contain personal data, logging systems must be integrated in order to ensure the traceability of operations relating to personal data, as it was able to recalled

in its recommendation on logging measures (deliberation no. 2021 of October 14, 2021). With regard to the scope of the processing operations concerned, the Ministry indicates that the draft order is primarily intended to cover processing implemented by the Infrastructure Networks and Information Systems Department (DIRISI), the exclusive purpose of which is the management of traces from certain information systems of the services under the responsibility of the Chief of Defense Staff, the General Directorate of Armaments and the General Secretariat for the administration of the Ministry. The implementation of this processing is authorized by an order of July 26, 2013 which was only published in the Official Armed Forces Bulletin, and which is intended to be governed by this order. In general, the Commission notes that the ministry's intention is that the draft decree that it submits to it for its opinion, if it is intended to cover the processing of the DIRISI, also makes it possible to set a legal framework for other data processing that meets similar characteristics. It notes that the Ministry intends to limit the vulnerabilities linked to the operation of a single trace management tool by encouraging the various staffs, directorates and services to implement their own trace management processing. In this perspective, the draft decree aims to regulate the trace management processing that the various entities of the ministry as well as the organizations attached to it could implement to ensure the security and defense of their respective information systems. .These elements recalled, the draft decree calls for the following observations. Issues the following opinion on the draft decree: On the purposes of the processing The purposes of the planned processing are to ensure the security and defense of information systems mentioned above and the information they contain, to ensure their management and operation and to identify irregularities in the access or use of these systems and the information they contain contrary to the legislative or regulatory provisions in force (for example, uses that do not comply with the rules and principles for using these systems). According to the details provided by the Ministry, this processing will also make it possible to carry out analyzes of the data collected, which may in particular lead to the pronouncement of sanctions against the agents responsible for the irregularities which have been observed or, more generally, to provide response to an incident occurring on an information system. The Commission observes that, even if the planned trace management processing will allow such analyses, the decisions relating to the agents which will be taken on the basis of the data are issued, will be in the context of separate processing, in accordance with the purposes of the latter. On the delimitation of the categories of data that can be recorded in the processing According to the terms of the draft decree, the processing of trace management is intended to regulate the collection and use of technical data relating to the traceability of the use of the information systems of the Ministry of the Armed Forces. On a preliminary basis, the Commission recalls that the

traceability data correspond, within the meaning of Article 101 of the law of January 6, 1978, to data relating to the collection, modification, consultation, communication (including transfers), interconnection and deletion operations relating to personal data. These data must make it possible to establish the reason, the date and the time of the operations of consultation and communication of the data and, as far as possible, to identify the persons who consult or communicate the data and the recipients of these. ci.Article 2 of the draft decree provides that trace management processing may include, in addition to traceability data (in particular IP address, URL address, date and time of connection to the information system), data identification (in particular surname, first name, registration number […]), authentication (in particular electronic certificate identifier, access token) as well as data allowing communication and exchanges (in particular subject of emails, naming elements files, file volume ). The list of data likely to be processed under each of these four categories is not exhaustive. The Ministry justifies this choice by the need to be able to cope with future technological developments, in a context of constant digital transformation. Without questioning this imperative, the Commission recalls that the processing of this data must not cause a disproportionate the privacy of the persons concerned. In this respect, it invites the Ministry to provide guarantees on the following points. Firstly, the concept of identification data is likely to be interpreted broadly and thus cover many categories of data. The Commission observes that the need to anticipate future technological developments cannot justify the absence of delimitation of the identification data likely to be collected. Therefore, the draft decree should either set an exhaustive list of data likely to be processed under this category, or, at the very least, exclude some of them. In this respect, the Commission takes note of the Ministry's commitment to explicitly exclude photography from the data collected as identification data. In any event, it invites the Ministry to limit the processing of data falling within this category to the data strictly necessary for the identification of the user whose trace is recorded.Secondly, with regard to data allowing the communication and exchanges mentioned in 4° of Article 2 of the draft decree, the Commission takes note of the ministry's commitment to amend this draft to expressly exclude the processing of the content of correspondence under this category of data. Furthermore, the data relating to exchanges and correspondence are likely to concern a large number of people including, in addition to the agents authorized to access the information systems of the ministry, the persons with whom these agents exchange e-mails. The Commission invites the Ministry to take the necessary measures to guarantee that only data relating to exchanges and correspondence relevant to the purposes of the processing will be kept. Finally, beyond the scope and volume of data that can be processed, the Commission considers that the information provided to the persons concerned by the processing of their

data must be regularly updated in order to precisely list the data likely to be collected. On the measures put in place to exclude the processing of sensitive data decree governing trace management processing cannot be the basis for the processing of sensitive data within the meaning of I of article 6 of the law of January 6, 1978, since such processing must be authorized by decree in Council of Statement taken after reasoned and published opinion of the Commission. In this case, the Ministry has implemented organizational measures to exclude the collection of such data, by ensuring that the planned processing does not collect the subject the name of files including a mention of the private nature of the correspondence. However, it is not excluded that this information contains sensitive data, without the sender having mentioned the private nature of the message. In this case, the Commission invites the Ministry to provide direct, regular and reinforced information to its agents as to the need to mention the private nature of their correspondence and to absolutely exclude the entry of sensitive data in their correspondence and their navigation. on the web. On retention periods Article 3 of the draft decree sets a maximum retention period for data of one year, before, if necessary, intermediate archiving for a period not exceeding five years from their registration . Firstly, the Commission recalls that the concept of intermediate archiving implies a necessary restriction of access to data. In this respect, it takes note of the ministry's commitment to modify article 3 in this sense and to specify the purposes concerned by archiving. Secondly, the draft decree provides that the health service of the armies retains the information and personal data that it processes in accordance with Article R. 6113-9-2 of the Public Health Code. According to the details provided by the Ministry of the Armed Forces, this provision was intended to meet the initial need to create a trace management processing specific to this service. Since this project has been discarded and DIRISI will use the traces produced by the information systems of the armed forces health service, the Ministry has undertaken to remove this provision, which the Commission takes note of. and recipients of processing dataArticle 4 of the draft decree lists the accessors and recipients of processing data. The Commission notes that only duly authorized public officials will be able to access the processing or be the recipients of the resulting data. It therefore observes that no transmission or access will be possible vis-à-vis other people, in particular any suppliers of solutions to which the ministry would have recourse (for example for level 3 support operations on equipment or systems) . On the information of the persons concerned The draft decree provides that the data controllers inform the persons concerned according to the procedures defined in article 116 of the law of January 6, 1978. The ministry specifies that a document recalling the rules in computer security, signed by each agent upon arrival, may be updated to include an information notice specific to the application of the decree governing trace management processing. In addition, this

order may be posted on the Ministry's intranet space. On the one hand, the Commission observes that certain agents will have, before the implementation of the processing operations, signed a document recalling the safety rules. This document therefore does not contain any information on the processing that will be implemented. It therefore invites the Ministry to inform these agents individually. On the other hand, the Commission considers that the information notices must be adapted to the specificities of the processing implemented in accordance with the regulatory act. Finally, persons other than the agents authorized to access the ministry's information systems could be affected by trace management processing. It is in fact not excluded, with regard to the processing of information relating to exchanges and correspondence, that personal data concerning the recipients or the authors of such communications (whether other agents or people outside the ministry) are processed. The Commission considers that measures to ensure that these people are kept informed should be implemented and observes that, with this in mind, the Ministry intends to insert an information notice on its website. As a preliminary point, although the provisions governing processing involving State security and defense do not require a privacy impact study to be carried out, the Commission considers that, with regard to the nature of the processing envisaged and of the number of persons potentially concerned, it is desirable that the Ministry carry out one in order to ensure that the conditions for implementing the processing effectively limit the risks to the privacy of the persons concerned. Firstly, the Ministry indicates that the proposed system will not allow modification of the raw data. This element, combined with the hardware and logical segregation of the trace management processing and the implementation of fingerprinting retained throughout the life cycle of the data, will ensure the integrity of the data. .Secondly, the Commission welcomes the fact that the Ministry has implemented authentication in accordance with its deliberation no. 2022-100 of July 21, 2022 adopting a recommendation relating to passwords and other shared secrets, in making mandatory two-factor authentication with smart card and password. Thirdly, stored data and communications will be encrypted with algorithms and key management procedures compliant with appendix B1 of the general security standard. Fourthly, the Commission notes that the operations carried out on the trace management processing implemented within the framework of this single regulatory act will themselves be subject to specific logging, and that the text provides that the data associated will be kept for a period of five years, which does not appear to comply with the Commission's recommendations. Unless the elements justify this duration and it is demonstrated that it makes it possible to reduce a significant residual risk, the Commission considers this duration to be disproportionate. In this respect, it takes note of the ministry's commitment to reduce this period to three years. Furthermore, it recommends that measures be implemented to

ensure the integrity of the logging data, in particular by implementing a policy of restricted access to this logging, different from that of the main processing. Finally, the Commission recalls that all the processing implemented on the basis of this order must comply with the same criteria in terms of data security as those presented to the Commission in the context of its referral.The president,

M. L. Denis