Deliberation 2021-122 of October 14, 2021Commission Nationale de l'Informatique et des LibertésNature of the deliberation: RecommendationLegal status: In force Date of publication on Légifrance: Friday November 05, 2021NOR: CNIL2132269XDeliberation No. 2021-122 of October 14, 2021 adopting a recommendation relating to loggingThe National Commission for Computing and Liberties, 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 data of a personal nature and on the free movement of such data, and repealing Directive 95/46/EC (GDPR); 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, investigation and prosecution in this area or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA; Considering the modified law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its article 8-I-2°-b), hereinafter data processing law and freedoms; report by Mr. François PELLEGRINI, commissioner, and the observations of Mr. Benjamin TOUZANNE, government commissioner; Adopts this recommendation: This deliberation constitutes a recommendation relating to the procedures for storing and using logging data. It aims to facilitate the compliance of the various controllers, and takes into account exchanges with stakeholders and the results of the consultation organized on this subject. This recommendation, and in particular the examples proposed therein, is neither prescriptive nor exhaustive and has the sole objective of helping the professionals concerned in their compliance process. ensure traceability of the access and actions of the various users authorized to access the information systems (and therefore the processing of personal data that these systems are likely to constitute). These devices can be backed either by applications (which are the software bricks specific to the processing implemented and are therefore subject to the implementation of so-called application logs), or by specific equipment (which are computer equipment associated with embedded software, subject to the implementation of so-called perimeter logs). This recommendation is applicable to logging devices linked to the application on which the processing is based and not to perimeter logging, which responds to a different logic. This recommendation applies to the implementation of logging devices. The analysis and recommendations contained in this document apply in the same way to a public or private body, and do not apply to processing operations whose main purpose would be logging itself. a logging device contributes to compliance with the obligation to secure all processing of personal data, pursuant to Articles 5 and 32 of the GDPR, as well as Articles 99 and 101 of the Data Protection Act for

processing subject to the Police-Justice Directive and, for processing subject to the Data Protection Act alone, Article 121 of this law. These devices may, in some cases, pursue other purposes (see below, section Other cases). They can in particular make it possible to document the transmissions of data to recipients, in order to satisfy the obligation for the data controller to be able to provide the persons concerned with information on the recipients or categories of recipients to whom the data concerning him have been communicated and on the information communicated to them (see in particular Article 15 of the GDPR and the decision of the Court of Justice of the European Union (CJEU), 7 May 2009, Rijkeboer, C-553/07, rec.). The retention period of the logs must then take into account this specific purpose, in compliance with the case law of the CJEU. The Commission stresses that this obligation of the data controller can also be satisfied by means other than logging devices. In this respect, it is necessary to find a balance between the security provided by logging, the monitoring that this type of system can create for authorized users and the emergence of particular risks linked to storage for too long. In the majority of cases, the logged data contains data relating to the persons concerned by the main processing. Consequently, the recording of this logging data does not modify the sensitivity of this processing, but can offer significant guarantees for the security of this data. However, these logs also contain data relating to authorized users of the system. This data may reveal information about these individuals, including information relating to their professional behavior. Care should be taken to limit the risks relating to these categories of people, by proportioning the collection, within the logs, of personal data relating to authorized users, to the sensitivity of the personal data of the main processing and to the risks that misuse of it would cause the persons concerned to run. This deliberation presents the recommendations of the Commission to find this balance according to different scenarios. GENERAL CASE The Commission recommends that the operations of creation, consultation, modification and deletion of personal data and information contained in the processing to which the logging is applied are the subject of a recording comprising the individually identified author, the timestamp, the nature of the operation carried out as well as the reference of the data concerned by the operation. In particular, duplication within the logs of the data concerned by the processing should be avoided. This logging can be integrated at the application level or managed at the technical level by means of the software resources used by the application. The Commission recommends keeping this data segregated from the main system. One method of implementation may consist of using physically separate equipment that is write-only accessible by the main processing applications, without the possibility of overwriting existing data. The granting of access rights to logging data should be subject to specific authorizations based on strict necessity. The Commission recommends that these data be kept for a

period of between six months and one year. It considers that this duration is sufficient, in most cases, to ensure a balance between, on the one hand, the need to have log data available to identify breaches of the processing system and, on the other on the other hand, the need not to keep too large a volume of data that could be the subject of attacks or misuse of purpose. The keeping of this traceability data is firstly justified by the objective of securing the processing. This security is essentially active: it is based on real-time or short-term use of this data to detect abnormal operations in order to counter attacks or intrusions, or to quickly remedy a computer incident by facilitating the identification of the problem. The Commission therefore recommends implementing a system for processing and analyzing the data collected and formalizing a process for generating alerts and processing them in the event of suspicion of abnormal behavior. This data can also be used ex post when a data breach (in particular by illegal consultation, transmission or use of data) is observed and the data controller is seeking to establish responsibility for it. Any reuse of the data collected for purposes other than that of securing the processing is likely to to constitute a misuse of purpose. The data controller should therefore implement the technical and organizational measures to limit this risk, for example by committing the persons accessing this data to respect a charter of use defining the acceptable uses of this data, or the raising of a specific alert in the event of modification access to the log data by an authorized account. The existence of logs copying some of the data contained in the file may lead, when this data is about to be deleted from the file, to keep them longer than their initial retention period. While this phenomenon is often unavoidable and acceptable given the role that these logging devices play in the security of the processing, the Commission recommends limiting this extension of the retention period as much as possible. The retention of traceability data should not lead data controllers to excessively retain personal data beyond that of the main processing. It also recommends minimizing the inclusion of personal data in log data. In any case, the data controller must define the methods to guarantee the confidentiality, availability and integrity of the logging data. In particular, the Commission recommends timestamping and signing the logs as soon as they are created. Similarly, the terms of use of the traces collected must in principle be the subject of formalized and documented rules and procedures. Users authorized to access the processing must be informed of the implementation of the logging system, the nature of the data collected and the retention period of the latter. This can for example be achieved via information notices presented at the time of authentication when accessing the processing. Insofar as logs are ancillary to a main processing operation and for the sake of clarity for data controllers, the Commission recommends that the rights of individuals, as described in Chapter III of the GDPR or in Chapter III of Title III of the Data Protection Act relating to logging, should be

exercised with the main controller. The Commission recommends that, when the processing of personal data to be subject to a logging measure is implemented, in in whole or in part, by a subcontractor within the meaning of the GDPR and the Data Protection Act, the subcontract provides for a logging obligation in accordance with this recommendation.Concerning registration in the processing register as provided by Article 30 of the GDPR or by Article 100 of the Data Protection Act, the Commission considers that this can be carried out in an alternative manner within e the entry in the register relating to the processing to which the logging is linked, or else in a specific entry in the register in the case of transverse logging and common to different processing operations. importance of the risk for individuals in the event of misuse of the purposes of the processing and the frequency of occurrence of such practices, the Commission considers that logging as described in paragraph 6 for a period of more than one year can also contribute to the internal control. The dissuasive capacity of such a process then contributes to the security of the processing, by limiting the risks of harm to the security of the main processing. A duration of more than one year can therefore contribute to constituting an appropriate guarantee of the protection of the privacy of the persons concerned with regard to the specific risks associated with this type of processing. To justify its use for this purpose, it is recommended that the data controller: demonstrates the risk, for the persons concerned by the main processing, linked to a diversion of the purpose of the use of the data concerning them. This point may be justified in particular by the fact that the planned or implemented processing processes sensitive or infringement data, on a large scale or leads to systematic monitoring of the persons concerned; has documented procedures for the analysis and internal investigations, on a regular basis and in the event of a report or suspicion of misuse of purpose. The Commission recalls that the implementation of such a traceability policy should not in principle lead the data controller to collect data presenting excessive risks of invasion of privacy for persons accessing or concerned by the connection logs, in particular sensitive data (as defined in paragraph 1 of article 6 of the Data Protection Act and in paragraph 1 of the 9 of the GDPR) or highly personal, when this data is not already present in the processing. It also recalls that the retention period Use of the logs must therefore be determined in a manner proportionate to the purpose pursued, in particular according to the timeframes described in the processes of the data controller. The data controller must also take into account the retention period of the processing data to determine a proportionate retention period for traces. In the most common cases, a maximum duration of three years may thus be justified. In any event, the Commission recalls that it is not possible to justify the retention period of traceability data by the sole limitation period for criminal offenses linked to the misuse of processing data by those who access it. OTHER CASESCertain

processing operations, regardless of the legal regime applicable to them, have specific characteristics which may justify an additional extension of the retention period for log data. They may, for example, correspond to: a legal obligation to keep traces for a specific period provided for by the texts; a specific purpose achieved using the log data, such as for example in the context of processing allowing the management of disputes to prove that the parties have indeed accessed the documents and procedural documents or to allow a certain transparency vis-à-vis the persons concerned; if necessary to be able to carry out post-attack or post-intrusion analyses, or following a suspicion of an attack linked to the evolution of knowledge of the threat in an automated data processing system. It is recommended that the data controller justifies, in a precise and documented manner, the reasons leading him to consider a longer duration, for example by relying on a particular legal obligation or particularities linked to the purpose pursued. The need to retain the data for a longer period may also be justified by the fact that this measure is the only way to deal with high risks for individuals in the context of a data protection impact assessment (AIPD) or an equivalent study. This analysis should be carried out on a case-by-case basis by applying the principles of the GDPR, and of the Data Protection Act where applicable, to determine the necessary guarantees in terms of security conditions, access and purposes of storage of this data. . Conversely, when the retention period for the personal data of the main processing operation is less than six months, it is recommended to adjust the practices to avoid retention of the processing data in the logs beyond the duration expected, while preserving the integrity of the logs. In practice, for this type of case, the Commission recommends not keeping personal data from the main processing in the logs. The log may retain only pseudonymous identifiers, or identifiers for which re-identification is particularly difficult. If this is not possible, it is also possible to set up procedures and tools for automatically purging the logs aimed at deleting from them the data from the main processing whose retention period has expired. Finally, it is reminded that, in application of the laws in force, the data of the connection logs may be the subject of a communication to certain authorized third parties, in particular within the framework of police investigations or criminal proceedings following a violation data. This recommendation concerns the logging measures applicable to generic processing; additional protection measures may be necessary for certain processing operations. The conduct of a DPIA is recommended to determine the appropriate additional measures. This deliberation will be published in the Official Journal of the French Republic. The President,M.-L. Denis