Deliberation 2022-005 of January 20, 2022Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Tuesday April 26, 2022NOR: CNIX2211330VDeliberation n° 2022-005 of January 20, 2022 providing an opinion on a draft decree amending Title IV of Book II of the Internal Security Code (request for opinion no. 21017956)The National Commission for Computing and Liberties, Seized by the Minister of the Interior of a request for Opinion on a draft decree amending Title IV of Book II of the Internal Security Code; Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its title III; Considering the decision of the Constitutional Council n° 2021-817 DC of May 20, 2021; Having heard the report of Mrs Sophie LAMBREMON, Commissioner, and the observations of Mr Damien MILIC, Deputy Government Commissioner, Issues the following opinion: Commission Nationale de l'Informatique et des Libertés (hereinafter "the Commission") received a draft decree from the Ministry of the Interior amending Title IV of Book II of the Internal Security Code (CSI ) relating to individual cameras by national police and gendarmerie officers. The Commission recalls that it has had the opportunity to rule on various occasions on the use of individual cameras for similar purposes. In particular, it has already ruled, in its deliberation no. 2016-385 of December 8, 2016, on decree no. 2016-1860 of December 23, 2016 relating to the implementation of the processing of personal data from individual cameras of national police officers and soldiers of the national gendarmerie. Article 45 of law no. CSI in order to integrate two new methods of consulting the recordings made by police officers and soldiers of the national gendarmerie by means of the individual cameras provided to them by their service: it will now be possible to transmit the images in real time at the command post and, in some cases, the personnel to whom the cameras are provided may have direct access to the recordings they make in the context of legal proceedings or intervention. This provision also specifies the conditions under which people are informed of the implementation of these cameras. Article L. 241-1 of the CSI mentions the purposes of the processing: the prevention of incidents during the interventions of police officers National Police and National Gendarmerie soldiers; the observation of offenses and the prosecution of their perpetrators by collecting evidence; the training and education of agents. If the purposes are not limited to the prevention of incidents during interventions, it should be remembered that recording can only be triggered during an intervention "when an incident occurs or is likely to occur, given the circumstances of the intervention or the behavior of the persons concerned", which constitutes a guarantee essential to limit the taking of images in the public space by law enforcement officers. It results both from the purposes mainly for monitored by the systems and missions entrusted to national police and gendarmerie officers, that the planned processing falls under the

provisions of Directive (EU) 2016/680 of April 27, 2016 of the European Parliament and of the Council of April 27, 2016 relating to the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, as transposed in title III of the amended law of January 6, 1978. Article L. 241-1 of the CSI provides that the terms of application of title IV of book II of the same code and use of data collected are specified by a Conseil d'Etat decree, issued after the Commission's opinion. recorded by means of individual cameras by agents of the national police and gendarmerie at the command post of the service concerned and by the personnel involved in the conduct and execution of the intervention; in the context of legal proceedings or an intervention, it allows agents to whom individual cameras are provided to have direct access to the recordings they make; it modifies the list of users and recipients of personal data stored in the processing operations; it introduces new guarantees s with regard to the data collected and their storage conditions; it brings the regulatory provisions into compliance with the regulations relating to the protection of personal data and thus modifies the rights of individuals as well as the procedures for logging the operations carried out on processing. On the status of a single regulatory act of the draft d decreeThe Commission notes that the draft decree constitutes a single regulatory act, within the meaning of IV of article 31 of the amended law of 6 January 1978, allowing agents of the national police and gendarmerie to proceed, by means of cameras individual, to recordings which can be transmitted in time and providing for direct access to the images by the agents who carried out the recording. When the Commission receives a request for an opinion relating to a "single regulatory act" which, in application of IV of article 31 of the modified law of January 6, 1978, does not authorize a particular treatment but the implementation of treatments which "respond to the same purpose, relate to identical categories of data and have the same recipients or categories of recipients", the impact analysis relating to data protection (DPIA) must not relate to one or more particular processing operations envisaged at the time of the referral but assess the risks and determine the categories of measures likely to control them for all the processing authorized by the project and likely to be implemented after its entry into force, each processing then only being the subject of the sending of a "conformity undertaking" to the Commission. This overall DPIA or "framework" (see CE, int., 8 January 2019, No. 396340) may, where appropriate, be supplemented with DPIAs relating to specific processing operations that would have been carried out on the date of the referral. The Commission notes that one and the same DPIA relating to a set of similar processing operations was sent to it (the "framework" DPIA), in accordance with Article 90 of the law of 6 January 1978 as amended. real-time recordings and direct access to recordings by

agentsIn the first place, I of draft article R. 241-3 of the CSI provides that "the images captured and recorded by means of individual cameras can be transmitted in real time to the command post of the service concerned and to the personnel involved in the conduct and execution of the intervention, when the safety of the agents of the national police or the soldiers of the national gendarmerie or the safety of property and people is threatened " . The Commission notes that the terms used in I of draft article R. 241-3 of the CSI constitute a reworking of those used in article L. 241-1 of the CSI. commanding the real-time transmission of the recordings are multiple and depend on the assessment of the official or the soldier who is on the ground. Depending on the operational context, the transmission of images may also be required by the information and command center or the gendarmerie's operations and intelligence center (for example, during an intervention in a major brawl, to allow the command room to assess the reinforcements to be deployed, or an attack in progress to contextualize and obtain as much information as possible in order to optimize the management of the event). In this case, the transmission will be done "on order" by voice, by radio, or even by telephone, in cases where the command room or the head of the device considers that the situation requires a transmission of images in real time, to allow a better appreciation of the event and thus optimize its management (reinforcements, driving order, etc.). This retransmission can only be carried out by the wearer of the camera who presses a button on the device provided for this purpose, and not by the authority which gave the order. The Commission notes that it is specified in I article 3 of the draft decree that the "security of agents, property or people is deemed to be threatened when there is an immediate risk to their integrity". It notes that the Ministry does not wish to limit the security of officers to threats to their physical integrity alone, insofar as their security must also be deemed to be threatened when there is an immediate risk of harm to their moral or psychological integrity. . It stresses, however, that the criterion laid down by the decree may correspond to a large number of situations, the need to resort to registration being assessed on a case-by-case basis. In this regard, it considers that the risk of harm to their integrity should be limited to the risk of serious harm. The Ministry indicates that each data controller will define, in the doctrines of use, criteria and use cases to determine the cases where the real-time transmission of images is necessary. The Board considers that types of situations and threats, as well as objective criteria for characterizing the risk, will have to be determined in the doctrine of use. In addition, the Commission recommends that this doctrine of use be defined at ministerial level and not at the level of each data controller. Secondly, II of draft article R. 241-3 of the CSI provides that, in Within the framework of a legal procedure or an intervention, the agents to whom the individual cameras are provided can have direct access to the recordings they make in order to facilitate the search

for perpetrators of offences, the prevention of imminent attacks on the public order, assistance to persons or the faithful establishment of the facts during the reports of interventions. In its decision n°2021-817 DC of May 20, 2021, the Constitutional Council considered that these provisions cannot only as implying that the integrity of the recordings made as well as the traceability of all their consultations are guaranteed, until they are erased. The decree recalls these obligations, which must be the subject of particular attention during the implementation of these texts. On the data collected Article 3 of the draft decree modifies article R. 241-2 of the CSI which indicates the personal data and information that may be recorded in the processing. Firstly, the Commission notes that the planned modifications introduce new guarantees with regard to the data collected, insofar as it is specified in Article R 241-2 of the CSI that, if “sensitive” data, within the meaning of I of article 6 of the modified law of January 6, 1978, can be collected, it is with the exception of genetic data and biometric data . It is also provided that it is prohibited to select a particular category of persons in the processing operations on the basis of these data alone.Secondly, if the extracted recordings are used for judicial, administrative or disciplinary purposes, the Commission takes note that there will be no automated links or interconnections with other processing of personal data. It asks that this guarantee be specified in the draft decree.Thirdly, it appears from the AIPD that areas of free field will exist in the processing with regard to the name of the file, the nomenclature of which is defined by the doctrine of use, an "observation" section for each downloaded video and a "note" section for each video extraction. comments" and "note". With regard to the "observations" field, the ministry indicated that this field can pursue three objectives: operational, training and technical purposes. With regard to the "note" field, the ministry indicated that this field makes it possible to indicate at what point in the video a specific event takes place, in order to allow the viewer to quickly go to the relevant sequence without watching the whole recording which can, in some cases, be very long. It also makes it possible to note the references of the procedure for which the extraction was made, and possibly to draw the attention of a service to the fact that another service has requested the extraction of the same images.The Commission takes note that this information cannot be saved in the form of drop-down menus and that the employment doctrines will specify the prohibition of entering personal data in these sections, the number of characters of which will be limited. that these free fields could also be pre-populated with specific information relating to the way in which they should be filled in and recalls that strict control must be ensured in this regard. In any case, the Commission requests that these fields can not be informed by the agents carrying the camera who have direct access to the recordings. The other planned modifications do not call for observation on the part of the Commi ssion.Under these conditions, the Commission considers

that the data processed are adequate, relevant and not excessive with regard to the purposes pursued.On accessors and recipientsThe Commission recalls that it follows from Article L. 241-1 of the CSI that the agents of the national police and the soldiers of the national gendarmerie who will have been equipped with individual cameras will be empowered, during legal proceedings and interventions, to make recordings, under the conditions provided for by law. The draft article R. 241-3-1 of the CSI specifies the persons who will be able to directly access the recordings of the processing or be their recipients. need to know: the head of the service or the commander of the unit (1° of I of draft article R. 241-3-1 of the CSI); agents or soldiers individually designated and authorized by the head of the department or the commander of the unit (2° of I of draft article R. 241-3-1 of the CSI). The Commission considers that 1° and 2° of I of draft article R. 241-3-1 of the CSI should specify the departments and units concerned. It takes note of the ministry's commitment to specify the provisions of this article as follows: "the head of the police service or the commander of the gendarmerie unit". With regard to the recipients, the Commission first recalls that, in the absence of specific purposes mentioned with regard to them, the data may only be transmitted to them for the purposes of the processing, as recalled in point 4 of this opinion. 3° of III of draft article R. 241-3-1 of the CSI includes, among the recipients, agents participating in the exercise of disciplinary power. The Commission notes that these agents are the heads of service and heads of unit who are empowered to intervene in the disciplinary aspect. It considers that the draft decree could be clarified on this point and takes note of the ministry's commitment to supplement the draft decree. Finally, the Commission notes that magistrates are not listed as recipients. The Government considers that they do not have to be included, since the latter are considered as authorized third parties. In this respect, the Commission recalls that authorized third parties, such as magistrates, are effectively authorized to receive communication of personal data in the context of an investigation mission. However, as recalled in recital 22 of Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 mentioned above, this communication must take place at the request of the authorized third party, a request which is in principle written, reasoned and precise. The Commission invites the Government to consider the existence of broader communication of images to magistrates, on the initiative of the services using the cameras in question, and not only at the request of a magistrate, in which case the magistrates could have intended to appear in the list of recipients.On data transfers outside the European UnionIt emerges from the AIPD that the data recorded in the processing may be communicated, in a non-automated manner, to international cooperation bodies in terms of judicial police as well as to the equivalent services or to the police services of a foreign State when these represent a sufficient level of protection of the

privacy, freedoms and fundamental rights of individuals with regard to the processing of which this data are or may be the subject. The Commission notes that, in the context of judicial cooperation, the images could be transmitted to countries third parties outside the European Union, within the framework of Interpol, but also within the framework of bilateral exchanges. According to the ministry, international police cooperation tools, in particular through national central offices (NCBs), allow the transfer of data internationally through secure messaging. In addition, in accordance with Article L. 235-1 of the CSI, the recordings of individual cameras may be communicated in a non-automated manner to international cooperation bodies in the field of judicial police as well as to counterpart services or to police services. of a foreign State when these represent a sufficient level of protection of the privacy, freedoms and fundamental rights of individuals with regard to the processing to which these images are subject or may be subject.The Commission recalls that transfers of data to States that do not belong to the European Union can only be carried out subject to compliance with the conditions set out in article 112 of the law of January 6, 1978 as amended. Where appropriate, appropriate safeguards for the protection of personal data should in particular be provided by a legally binding instrument. In the absence of an adequacy decision adopted by the European Commission or of appropriate guarantees, and by way of derogation from the aforementioned article 112, such transfers can then only be carried out subject to compliance with the conditions set out in article 113. of the law of January 6, 1978 as amended. On the rights of the persons concerned With regard to the information of the persons concerned, the Commission notes that Article L. 241-1 has organized a special system, by providing for oral information, except exception, when the recording is triggered, supplemented by general information for the public on the use of these individual cameras. The decree provides that this information is given on four national websites. The Commission invites the Government, on the one hand, to provide in this general information all the information mentioned in Article 104 of the "Informatique et Libertés" law, supplemented by all information useful to the public and, on the other hand, to provide also information on the websites of decentralized administrative services, such as those of the prefectures. It recalls that this provision, while it does not provide for the information to be provided individually to each person in the event of direct collection, requires the data controller to "make it available" to persons, permanently and without their request. go. It therefore draws attention to the fact that the wording of the decree according to which the right to information "is exercised with" the administration seems inappropriate. In this regard, it takes note of the ministry's commitment to add an III to article R. 241-16 of the CSI in order to indicate that "The information provided for in the provisions of article 104 of the same law is made available to the persons concerned".

Furthermore, the Commission notes that the ministry does not intend to make any general and permanent restriction on the right to information of the persons concerned. paragraph 4 of article L.241-1 of the CSI. Thus, the information will be delivered orally to the persons concerned by the agent before the triggering of the camera unless: the situation gives reason to fear an immediate risk of harm to the life or integrity of a person; the agents act within the framework of Article 73 of the Code of Criminal Procedure (flagrant crime or offence); the person concerned has fled and does not return to the scene of the intervention. However, the Commission emphasizes that the Constitutional Council, in its decision of May 20, 2021 mentioned above, noted that if article L. 241-1 of the CSI allows that the triggering of the recording may, by exception, not be the subject of this information when "the circumstances prohibit ", these circumstances cover the only cases where this information is " made impossible for purely material reasons and independent of the reasons for the intervention ". Under these conditions, the Commission requests that the Ministry expressly limit the cases in which the recording is carried out without the knowledge of the person concerned only to cases in conformity with the aforementioned decision. If this seems to be the case of an immediate risk of harm to the integrity of a person or an escape of the individual filmed, she wonders about the inclusion of the criterion of flagrance. It considers that the draft decree should include the criteria taken from the decision of the Constitutional Council, which could then be specified in the employment doctrine drawn up by the ministry. The Commission notes that there will be no right for individuals to request the triggering of the cameras and that the latter can only be triggered within the framework of the provisions of Article L. 241-1 of the CSI. Furthermore, it notes that it appears from the AIPD that, if the intervention so requires, a "security" mode may be activated by the agent carrying the camera, thus deactivating the lights and the sound signal for more discretion. On this point, the ministry indicates that the recording is also interrupted by the triggering of this mode, and therefore considers that the information of the persons would not be required. However, the Commission notes that the use of the "security" mode activates the recovery of the 30 seconds of buffer memory preceding its activation and that there will indeed be a processing of personal data by the activation of this mode. Therefore, the persons concerned must be informed. It recalls that the Constitutional Council has only accepted the possibility of not informing people for purely material reasons. The Commission therefore requests the removal of this "safety" mode. On the security measures The Commission notes that the device only works with specific professional smartphones, called "NEO" (New Operational Equipment), which are subject to specific security measures. The ministry indicates that the data (images, sound and metadata) are encrypted on the device, then during their transfer and then again during storage, and this by means of

algorithms in accordance with appendix B1 of the general security reference system (RGS). The choice of these piece ciphers implies that the data will be manipulated in the clear at several stages. The Commission notes that the Ministry has taken organizational measures (in particular access control by strong authentication on the camera and access logging) to limit the risks of breaches of confidentiality. Given the nature of the data processed, it strongly encourages the Ministry to monitor the possibilities of changes to the system envisaged in order to eliminate these intermediate decryption steps which are not justified by the need to view the data. Furthermore, the Commission stresses the importance of the robustness of the key management mechanisms in order to take advantage of the level of security that these ciphers can provide. It recalls that it considers the mechanisms described in appendix B2 of the RGS as defining the state of the art in this area, and considers it necessary that they be effectively implemented by the ministry. Finally, it recommends auditing the key storage mechanisms (in particular on the device) in order to ensure their robustness and the difficulty for a third party to circumvent the encryption. In the context of an export carried out in Legally, the extracted file must be manually deleted from the computer on which the extraction is made. The Commission notes that a control of these deletions will be carried out periodically by the administrator. It considers that a mechanism (technical or organisational) making it possible to ensure that the periodic control by the director does in fact take place should be implemented. In addition, it recommends that the Ministry, in the medium term, study alternative and more reliable solutions that would make it possible to automate this deletion. In any event, it reminds the Ministry of its obligation to ensure this effective deletion within the defined deadlines. The Commission notes that a password authentication mechanism corresponding to its minimum recommendation is provided for the connection management software or in the command room. Given the sensitivity of the data, it recommends that the ministry strengthen this authentication policy. Authentication by agent card could, for example, meet this recommendation. On logging, the Commission considers it necessary to distinguish between two types of traces: firstly, the metadata: the personnel number ("RIO") of the bearer, the , application traces are generated at the level of the video management software in order to trace the operations carried out as well as the reason justifying these operations. The Commission recalls that the processing of these data is, in principle, for the sole purpose of detecting and preventing illegitimate operations on the main data. The Commission notes that specific means of control, whether by the direct hierarchical authority or by the data protection and governance audit office of the General Inspectorate of the National Gendarmerie on the one hand, and by the services of the General Inspectorate of the National Police on the other hand, are planned. However, it considers it necessary to provide for

organizational measures to supplement this one-off verification with periodic and systematic verification (for example, by implementing an annual trace review) in order to make use of this data and contribute to the detection of abnormal behavior. Under these conditions, the targeted retention period of six years appears excessive, particularly insofar as no systematic proactive valuation of the traces is implemented and no specific risk of breach of security is identified justifying such a duration. The Commission therefore considers that this duration should be reduced. For information, a period of three years has been considered proportionate by the Commission in similar cases. Subject to the above observations, the security measures described by the data controller seem to comply with the security requirement provided for in Article 4-6° of the amended law of 6 January 1978. The Commission recalls, however, that this obligation requires updating the AIPD and its security measures with regard to the regular reassessment of the risks. The President Marie-Laure DENIS