Deliberation SAN-2021-003 of January 12, 2021 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Thursday January 14, 2021 Deliberation of the restricted committee n°SAN-2021-003 of 12 January 2021 concerning the Ministry of the InteriorThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Messrs Alexandre LINDEN, president, Philippe-Pierre CABOURDIN, vice-president, and Mesdames Anne DEBET and Christine MAUGÜE, members; Having regard to Convention No. 108 of the Council of Europe of 28 January 1981 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 April 27, 2016 on the protection of personal data and the free movement of such data; Having regard to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 a April 2016 on 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 penalties, and the free movement of such data; Having regard to law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its articles 20 and following; Having regard to decree no. 2019-536 of May 29, 2019 taken for the application of law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms; Having regard to deliberation no. 2013-175 of July 4, 2013 adopting the Commission's internal regulations Commission Nationale de l'Informatique et des Libertés; Having regard to decision no. lines ments implemented by the Ministry of the Interior or on its behalf; Having regard to the decision of the President of the National Commission for Computing and Freedoms appointing a rapporteur to the restricted committee, dated October 2, 2020 ;Having regard to the report of Mrs. Sophie LAMBREMON, reporting commissioner, notified to the Ministry of the Interior on October 30, 2020;Having regard to the written observations submitted by the Ministry of the Interior on December 1, 2020;Having regard to the oral observations made during the meeting of the Restricted Committee, on December 10, 2020; Having regard to the other documents in the file; Were present at the Restricted Committee meeting: - Mrs. Sophie LAMBREMON, commissioner, heard in her report; As representatives of the Ministry of Interior:- […];- […];The Ministry of the Interior having the floor last;The Restricted Committee adopted the following decision:I. Facts and procedure1. Following the confinement decided by the Government in March 2020, several press articles reported on the use, by the police forces (in particular the Cergy-Pontoise police station) and the gendarmerie (in particular the gendarmerie group department of Haute-Garonne), drones equipped with a camera to ensure compliance with the measures taken in this context. The use of such drones appearing to her to be likely to implement the

processing of personal data, the President of the National Commission for Computing and Liberties (hereinafter the CNIL or the Commission) sent a letter dated 23 April 2020, asked the Ministry of the Interior for details on the processing carried out in this context.2. In the absence of a response, the President of the Commission, by decision no. 2020-076C of May 7, 2020, initiated a review procedure against the ministry. The purpose of this procedure was to verify compliance by the Ministry of the Interior with all the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the Regulation or the GDPR ), law no. 78-17 of January 6, 1978 as amended relating to data processing, files and freedoms (hereinafter the law of January 6, 1978 or the Data Protection Act), directive (EU) 2016/ 680 of the European Parliament and of the Council of April 27, 2016 (hereinafter the police-justice directive) and the provisions provided for in articles L251-1 and following of the internal security code. As part of this procedure, the President of the Commission, on 8 May 2020, sent to the Ministry of the Interior, the Paris police headquarters, the Cergy-Pontoise police station and the Haute -Garonne questionnaires on the use of drones in order to enforce the containment measures deployed as part of the state of health emergency. The Ministry of the Interior responded to all of these questionnaires by letter dated May 27, 2020.3. On July 9, 2020, a CNIL delegation visited the premises of the Paris police headquarters to carry out an on-site check. This control notably enabled the control delegation to carry out a test flight of a drone used by the Paris police headquarters.4. Various exchanges took place by e-mail between the ministry and the control delegation between July and September 2020. These exchanges concerned the transmission of documents requested during the control as well as clarifications requested later.5. For the purpose of examining these elements, the President of the Commission, on October 2, 2020, appointed Mrs. Sophie LAMBREMON as rapporteur, on the basis of Article 22 of the law of January 6, 1978.6. At the end of her investigation, the rapporteur, on October 30, 2020, served the Ministry of the Interior with a report detailing the breaches of the Data Protection Act that she considered constituted in this case. The rapporteur proposed to the restricted formation of the Commission to issue an injunction to bring the processing into compliance with the provisions of Article 87 of the Data Protection Act, as well as a call to order. It also proposed that this decision be made public and no longer allow the ministry to be identified by name after the expiry of a period of two years from its publication.7. On the same day, the Ministry of the Interior was informed that this file was on the agenda of the restricted training session of December 10, 2020.8. On December 1, 2020, the department filed observations.9. The Ministry and the rapporteur presented oral observations during the session of the Restricted Committee.II. Reasons for decisionA. On the existence of personal data processing10. The rapporteur observes that the Paris

police headquarters, the Cergy-Pontoise police station and the Haute-Garonne departmental gendarmerie group have used drones to verify compliance with containment measures. In addition, the Paris police headquarters has also used these devices for other purposes, such as judicial police missions (reconnaissance of a place before an arrest, surveillance of drug trafficking), maintenance operations order (surveillance of demonstrations) or crisis management and road checks (surveillance of urban rodeos).11. The rapporteur notes that the drones used are equipped with a camera capable of capturing high-resolution images and possessing zoom capabilities that can magnify the image between six and twenty times.12. With regard to these technical capacities, the rapporteur considers that the use of these drones by the Ministry of the Interior gives rise to the processing of personal data when people are filmed in conditions allowing their identification.13. The Ministry of the Interior, for its part, first asserted in response to the questionnaires sent by the President of the CNIL that the flight of the drones did not give rise to any processing of personal data, the persons not being identifiable. In his observations in response to the sanction report, he then considered that the legal uncertainty relating to the nature of the data processed demonstrated the administration's good faith, that in any event, the blurring system implemented excluded any processing of personal data, while specifying that technical considerations prevented this blurring system from being carried out at the level of the drone capturing the images and before any transmission thereof.14. The Restricted Committee considers that the qualification of personal data processing applies to a video capture system filming people for the following reasons.15. Firstly, on the existence of personal data processing, article 2 of the Data Protection Act provides: unless otherwise provided, in the context of this law, the definitions of article 4 of Regulation (EU) 2016/679 of April 27, 2016 .16. Under Article 4 of the GDPR, processing of personal data constitutes any operation or set of operations whether or not carried out using automated processes and applied to personal data or sets of data, such as the collection, recording, organization, structuring, storage, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of available, reconciliation or interconnection, limitation, erasure or destruction. This same article defines personal data as any information relating to an identified or identifiable natural person […]; an identifiable natural person is deemed to be a natural person who can be identified, directly or indirectly, in particular by reference […] to one or more specific elements specific to his physical, physiological, genetic, psychological, economic, cultural or social identity .17 . With regard to these definitions, the Restricted Committee notes that any operation – in particular the capture, transmission, modification or consultation – relating to the image of persons who can be recognized constitutes processing of personal data.18. The Restricted Committee

observes that this analysis, adopted a long time ago by the CNIL, has been enshrined in European case law since 2014: the image of a person recorded by a camera constitutes personal data within the meaning of the provision referred to in previous point insofar as it allows the data subject to be identified (CJEU, 11 December 2014, Ryneš, case C-212/13, point 22). It was recalled very recently by the European Data Protection Board (hereinafter the EDPS) in its guidelines 3/2019 of 29 January 2020 on the processing of personal data by video devices: Systematic monitoring and automation of a specific space by optical or audio-visual means, mainly for the purpose of protecting property or protecting human life and health, has become an important phenomenon of our times. This activity entails the collection and retention of pictorial or audiovisual information about all persons entering the monitored space that are identifiable on the basis of their appearance or other specific elements. The identity of these persons can be established on the basis of this information .19. With more specific regard to drones equipped with a camera, the urgent applications judge of the Council of State considered that the disputed surveillance device […] which consists of collecting data, thanks to the capture of images by drone, to transmit them, in certain cases, to the command center of the police headquarters for real-time viewing and to use them for the performance of administrative police missions constitutes processing (Council of State, order of May 18, 2020, nos 440442 and 440445). Noting that no system was put in place to prevent, in any case, that the information collected could lead to the identification of persons, this court concludes that the data likely to be collected by the disputed processing must be regarded as of a personal nature .20. Finally, in an opinion of September 20, 2020 relating to the use of airborne image capture devices by public authorities, the Council of State specified that, in view in particular of the technologies currently available and their development and the material means available to the public authorities, the Council of State considers that the images of persons captured by means of airborne cameras by these authorities in the context of public security or civil security missions must, in principle, be regarded as personal data and that, consequently, the collection and use of these images are subject to compliance with the texts recalled above. However, it could be different in the event of employment under special conditions excluding the existence of reasonable possibilities of identifying persons, or in the event that technical devices preventing identification are implemented (Council of State , interior section, session of Tuesday, September 20, 2020, no. 401 214).21. The Restricted Committee recalls that in this case, the Paris police headquarters, the Haute-Garonne departmental gendarmerie group and the Cergy-Pontoise police station have admitted having used drones equipped with a camera in the context of checks compliance with confinement measures and, for the Paris police headquarters, for other purposes, in particular judicial and law

enforcement. These drones flew at an altitude of between 30 and 120 meters, according to the actors, and were equipped with a 12 million pixel lens that could magnify the image between six and twenty times.22. The control delegation, having carried out a drone test flight on July 9, 2020, found that the technical characteristics mentioned above allow the identification of persons.23. Secondly, with regard to a possible blurring device which could make it possible to make the persons concerned unidentifiable, the Restricted Committee notes, first of all, that the Paris police headquarters, the departmental gendarmerie group of Haute -Garonne and the Cergy-Pontoise police station indicated, in their response to the questionnaires sent, that no blurring device had been put in place.24. It then observes that the Paris police headquarters subsequently indicated, during the check carried out on July 9, 2020, that a blurring device was under development. The Ministry of the Interior clarified, during the meeting of December 10, 2020, that its deployment had been effective since the end of August 2020.25. Consequently, the Restricted Committee notes, on the one hand, that such a device was not implemented during the flights mentioned in the questionnaires sent to the operational services, and that drones equipped with a camera therefore carried out numerous flights without blurring of the images collected before the deployment of the mechanism. It considers, on the other hand, that the device described during the present procedure cannot, however, exempt the images collected from the applicable regulations on the protection of personal data.26. Indeed, firstly, the blurring system mentioned does not apply to the images captured by the camera present on the drone and transmitted to the pilot of the drone. If the viewing of unblurred images by the pilot of the drone is easily explained by security imperatives (control of the device during flight time), which the restricted training does not call into question, the fact remains that the capture of unblurred images by the camera and their transmission to the pilot constitute personal data processing operations.27. Secondly, it follows from the responses provided by the police headquarters that it recorded unblurred images when using drones for the purposes of judicial police missions, which also constitutes data processing of a personal nature.28. Finally, and contrary to the statements made by the Ministry of the Interior during the session, it appears from the documents provided in defence, and more particularly from the note relating to blurring entitled Processing of video streams from drones, dated November 23, 2020, that the blurred flows can be consulted in plain text by the agents of the police headquarters: Since the blurring device is controlled by the DILT (direction of innovation, logistics and technologies), it is impossible for the DOPC (direction public order and traffic) to access non-blurred streams. Access to non-blurred streams would require a modification of the configuration currently implemented; only an engineer with the rights to the entire device can do this laborious work. Engineers with these rights are placed under a different command

from that of the DOPC. The Restricted Committee deduces from this document that, although laborious, access to unblurred flows remains possible by persons placed under the responsibility of the data controller. Therefore, the processing must be qualified as processing of personal data.B. On the identification of the data controller29. The Restricted Committee emphasizes that all of the processing covered by this procedure, the purpose of which is to ensure compliance with the containment measures adopted in the context of the state of health emergency, to intervene for the benefit of missions of judicial police, law enforcement missions, or in the context of crisis management or roadside checks, fall under the jurisdiction of the Ministry of the Interior, in accordance with the provisions of Decree No. 2017-1070 of May 24, 2017 relating to the powers of the Minister of the Interior, which provides the Minister of the Interior prepares and implements the Government's policy in terms of internal security, public freedoms, territorial administration of the State, immigration, asylum and road safety .30. It also points out that the services concerned (grouping of the departmental gendarmerie of Haute-Garonne, police station of Cergy-Pontoise and police headquarters of Paris) all act under the supervision of the Ministry of the Interior.31. The Ministry of the Interior does indeed consider itself to be the data controller, its central services having moreover drafted a command instruction providing for the use of drones, particularly in the context of confinement.32. Therefore, the Restricted Committee holds that the latter must be considered the data controller concerned by this procedure.C. On the applicable law33. The first paragraph of article 87 of the Data Protection Act, first article of title III of the law, provides: this title applies, without prejudice to title I, to the processing of personal data implemented, for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the protection against threats to public security and the prevention of such threats, by any authority competent authority or any other body or entity entrusted, for the same purposes, with the exercise of public authority and the prerogatives of public power, hereinafter referred to as the competent authority .34. This Title III therefore applies to processing that meets a dual characteristic relating to its purpose, on the one hand, and to the quality of the data controller, on the other hand.35. With regard to the purposes pursued by the processing resulting from the flights of drones equipped with a camera, it appears from the declarations made by the departmental gendarmerie group of Haute-Garonne, by the police station of Cergy-Pontoise and by the police headquarters of Paris that the images were used, by these three actors, in order to ensure compliance with the containment measures adopted within the framework of the state of health emergency and, for the last of them only, to other purposes, such as judicial police missions, law enforcement, crisis management and roadside checks.36. The Restricted Committee considers that the aforementioned

missions fall within the scope of the purposes referred to in Article 87 of the Data Protection Act, either because they aim to prevent or detect criminal offenses - for example, when drones are used to to ensure compliance with containment or traffic control measures –, to investigate or prosecute in criminal matters – for example for judicial police missions – to protection against threats to public security and the prevention of such threats – for example for law enforcement or crisis management missions.37. The Restricted Committee also considers that, within the framework of these missions, the Ministry of the Interior must be regarded as the competent authority, with regard to Article 1 of Decree No. 2020-874 of July 15, 2020 relating to the powers of the Minister of the Interior (previously decree no. 2017-1070 of 24 May 2017), cited above.38. Consequently, the Restricted Committee considers that in this case, the processing implemented by the Ministry of the Interior for the various purposes mentioned above must comply with the provisions of Title III of the Data Protection Act.D. On breaches1. On the breach relating to the legality of the processing and the absence of an impact study39. The second paragraph of article 87 of the Data Protection Act provides that the processing referred to in Title II of the law is only lawful if and insofar as it is necessary for the performance of a mission carried out, for one of the purposes set out in the first paragraph, by a competent authority within the meaning of the same first paragraph and where the provisions of Articles 89 and 90.40 are complied with. Under the terms of I of Article 89 of the law, if the processing is carried out on behalf of the State for at least one of the purposes set out in the first paragraph of Article 87, it is provided for by a legislative or regulatory provision taken under the conditions provided for in I of Article 31 and Articles 33 to 36. Pursuant to II of the same article, if the processing relates to data covered by article 6 of the law (known as sensitive data), it must be provided for by a legislative or regulatory provision taken under the conditions provided for in II of the article 31. Article 31 of the law to which reference is made requires that the processing of data in question be authorized by order of the competent minister or ministers, issued after a reasoned and published opinion from the Commission and, in the event of processing of sensitive data, by a Conseil d'Etat decree following a reasoned and published opinion from the CNIL.41. Article 90 of the law provides: if the processing is likely to create a high risk for the rights and freedoms of natural persons, in particular because it concerns data mentioned in I of Article 6, the controller of processing carries out an impact analysis relating to the protection of personal data .42. As a preliminary point, the Restricted Committee notes that the Ministry of the Interior does not contest the characterization of this failure, having wrongly considered that the processing in question did not concern personal data.43. With regard to the provisions of Article 89, the Restricted Committee notes that no legislative or regulatory framework authorizes and regulates the processing of personal

data resulting from the use by the Ministry of the Interior of drones equipped with a camera. By indicating that work is underway to draw up a legal framework as soon as possible, the Ministry of the Interior confirms this point.44. With regard to the provisions of Article 90, the Restricted Committee considers that the processing implemented in this case is likely to create a high risk for the rights and freedoms of the persons concerned. This high risk arises, on the one hand, from the characteristics of drones, which are flying objects carrying a camera capable of filming in high resolutions, anywhere and at any time. They are therefore able to film anyone circulating in public space, follow them and process intangible personal data such as their facial features. The risk arises, on the other hand, from the use made of drones by the Ministry of the Interior, in particular during demonstrations, occasions during which the political opinions, religious or philosophical convictions of people, or their trade union membership, are likely to be revealed. Finally, the risk is aggravated by the fact that the processing operations are potentially implemented without the knowledge of the people, who are often not aware of the presence of drones, the activation of the camera and the recording of their image. This risk is in this respect aggravated, in the present case, by the lack of information of the persons on the occasion of the flights carried out.45. The Restricted Committee notes that Article 90 of the Data Protection Act specifies that this risk may also arise due to the use of new mechanisms, which is indeed the case here.46. Consequently, the Restricted Committee considers that the use of drones equipped with a camera gives rise to a high risk for the rights and freedoms of natural persons and that, therefore, it was up to the Ministry of the Interior to carry out an analysis of impact relating to the protection of personal data.47. The Restricted Committee notes that no impact assessment has been carried out.48. It appears from all of these elements that the conditions for the lawfulness of the processing implemented are not met. The Restricted Committee therefore considers that breaches of Articles 89 and 90 of the Data Protection Act have been constituted.2. On the breach relating to the information of persons Under the terms of article 104 of the Data Protection Act, the data controller provides the data subject with the following information: 1° The identity and contact details of the data controller processing and, where applicable, those of his representative; 2° Where applicable, the contact details of the data protection officer; 3° The purposes pursued by the processing for which the data are intended; 4° The right to introduce a complaint to the Commission Nationale de l'Informatique et des Libertés and the contact details of the commission; 5° The existence of the right to request from the data controller access to personal data, their rectification or erasure, and the existence of the right to request a limitation of the processing of personal data relating to a data subject .49. As a preliminary point, the Restricted Committee notes that the Ministry of the Interior does not dispute the characterization of

this breach, merely recalling the commitments made to ensure, in the future, that the persons concerned are informed.50. The Restricted Committee notes that the Haute-Garonne departmental gendarmerie group and the Cergy-Pontoise police station indicated, in their response to the questionnaire sent, that people were informed of the presence of the drone by a voice message inviting them to disperse. . The Paris police headquarters indicated that no specific information system had been put in place.51. It appears from the responses provided that no information meeting the requirements of Article 104 of the Data Protection Act has been communicated to the persons concerned.52. The Restricted Committee notes that, if Article 107 of the Data Protection Act allows, under certain conditions, restrictions on the rights of individuals and in particular the right to information, these restrictions must be provided for by the act establishing the processing . In the present case, in the absence of any act establishing the processing operations in question, no limitation of the right to information could be provided for.53. It appears from all of these elements that the information provided to people, when it existed, did not meet the legal requirements. The Restricted Committee therefore considers that a breach of Article 104 of the Data Protection Act has been established.III. On corrective measures and their publicity54. Under the terms of III of article 20 of the law of January 6, 1978: When the data controller or its subcontractor does not comply with the obligations resulting from regulation (EU) 2016/679 of April 27, 2016 or from this law , the President of the National Commission for Computing and Liberties may also, if necessary after having sent him the warning provided for in I of this article or, if necessary in addition to a formal notice provided for in II, seize the restricted formation of the commission with a view to the pronouncement, after adversarial procedure, of one or more of the following measures: 1° A call to order; 2° An injunction to bring the processing into conformity with the obligations resulting of Regulation (EU) 2016/679 of 27 April 2016 or of this law or to satisfy requests submitted by the data subject with a view to exercising their rights, which may be combined, except in cases where the processing is implemented by the State, a penalty payment have the amount cannot exceed €100,000 per day of delay from the date set by the restricted committee; (…) .55. The rapporteur proposes to the restricted committee that a call to order be issued as well as an injunction to bring the processing into compliance with the provisions of the Data Protection Act. It also proposes that this decision be made public.56. In defence, the Ministry of the Interior considers that the pronouncement of a corrective measure is not justified, a formal notice seeming to it sufficient in this case, and that the publicity of the possible measure to be taken does not appear necessary. Lastly, he considers that an injunction to cease the use of drones is not an option, as such use now constitutes an undeniable operational necessity.57. The Restricted Committee considers that, in the present case, the aforementioned

breaches justify a call to order against the Ministry of the Interior for the following reasons.58. The Restricted Committee notes the seriousness of the breach relating to the lawfulness of the processing, this breach depriving all the processing implemented of a legal basis. It also emphasizes that the persons concerned were deprived of all the guarantees which they should have enjoyed, in particular information relating to the processing and the exercise of their rights.59. It also notes the significant risks for the rights and freedoms of individuals, mentioned above, linked to the possibility offered by these new systems of identifying any person circulating in the public space, including in circumstances that may reveal particularly sensitive information, for example linked to their political opinions, their religious or philosophical beliefs or their trade union membership.60. It also notes that technological developments are making drones more and more discreet with increased capture capabilities of their cameras which give the Ministry of the Interior the possibility of flying its drones at increasingly high altitudes, while retaining a high-precision image. People are therefore unlikely to become aware of the processing carried out and the capture of their image.61. Finally, the Restricted Committee considers that the improvement of technologies such as facial recognition could lead, in the future, to even greater risks for individual rights and freedoms if they were coupled with the use of drones. It therefore considers that their deployment outside any legal framework should be severely sanctioned.62. The Restricted Committee considers that the aforementioned elements also make it necessary for an injunction to be issued. In addition, since the ministry indicated during the meeting that it did not intend to give up, even temporarily, on the use of drones equipped with a camera, the issuance of an injunction constitutes the appropriate measure to bring it to use drones for this purpose only when a legal framework authorizing it has been adopted.63. Finally, and for the same reasons, the Restricted Committee considers it necessary that its decision be made public. It notes, on this point, that the public has demonstrated, in recent months, a legitimate interest in matters relating to the processing of its personal data by the State. The publication of a sanction decision by the authority specifically responsible for the protection of personal data thus appears fully justified. order for breaches of Articles 89, 90 and 104 of the Data Protection Act; issue an injunction against the Ministry of the Interior to bring the processing in question into conformity with the obligations resulting from Article 87 of the Data Protection Act, and in particular: o for purposes covered by Title III of the Data Protection Act, only resort to capturing personal data from drones after the adoption of a framework re normative authorizing the processing of such data; make public, on the CNIL website and on the Légifrance website, its deliberation, which will no longer identify the ministry by name at the end of a period of two years from its publication. Chairman Alexandre LINDEN This decision may be appealed to the Council of State within two months of

its notification.