Deliberation 2018-354 of December 13, 2018Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Wednesday May 08, 2019NOR: CNIX1909667XDeliberation n° 2018-354 of December 13, 2018 providing an opinion on a draft decree amending decree no. 2018-383 of 23 May 2018 authorizing the processing of personal data relating to the monitoring of people in psychiatric care without consent (request for opinion no. 18020552)The National Commission for Informatics and of freedoms, Seizure by the Minister of Solidarity and Health of a request for an opinion concerning a draft decree in the Council of State modifying decree n ° 2018-383 of May 23, 2018 authorizing the processing of personal data relating to the monitoring of persons in psychiatric care without consent; Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing personal data; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; Having regard to Directive 2016-680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purposes of the prevention, investigation, detection and prosecution of criminal offenses or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA; Having regard to the Code of Criminal Procedure, in particular its article 706-135; Having regard to the Public Health Code, in particular its articles L. 1110-4, L. 3212-1, L. 3213-1, L. 3213-7, L 3214-3 Having regard to Law No. 78-17 of January 6, 1978 as amended relating to computer e, to files and freedoms; Considering the decree n° 2005-1309 of October 20, 2005 modified taken for the application of the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms; Having regard to the decree of March 5, 2015 creating an automated processing of personal data called the Report processing file for the prevention of terrorist radicalization (FSPRT); Having regard to decree no. 2018-383 of May 23, 2018 authorizing the processing of personal data relating to the monitoring of people in psychiatric care without consent; Having regard to instruction no. SG/2016/14 of 8 January 2016 relating to the framework for intervention of regional health agencies with regard to the phenomena of radicalization; Having regard to instruction no. SG/2016/377 of 2 December 2016 relating to the implementation of the territorial strategy of the Ministry of Social Affairs and Health by the ARS in the context of prevention and management of the radicali ation; Having regard to deliberation no. 2018-152 of 3 May 2018 giving an opinion on a draft decree authorizing the processing of personal data relating to the monitoring of people in psychiatric care without consent;

Having regard to the file and its supplements; After having heard Mr. Alexandre LINDEN, commissioner, in his report and Mrs. Nacima BELKACEM, government commissioner, in her observations, Issues the following opinion: The Commission has received a request for an opinion from the Minister for Solidarity and Health amending Decree No. 2018-383 of May 23, 2018 authorizing the processing of personal data relating to the monitoring of people in psychiatric care without consent. These treatments, called HOPSYWEB and managed by the regional health agencies (ARS), are intended to ensure at the departmental level the follow-up of people in psychiatric care without consent taken care of in application of articles L. 3212-1, L. 3213-1, L. 3213-7, L. 3214-3 of the Public Health Code and Article 706-135 of the Code of Criminal Procedure. The planned changes aim to link HOPSYWEB processing with the FSPRT and thus allowing in particular the prefects of the department and, in Paris, the prefect of police of the place of hospitalization to be informed, for the purposes of preventing radicalization, of the possible hospitalization without consent of a person who would also be registered in the FSPRT. If the planned interconnection should make it possible, in a general context of preventing the risks linked to the radicalization of people with psychiatric disorders, to improve the methods of transmitting information to the prefects relating to admissions to psychiatric care without consent, the Commission emphasizes the profound difference in purpose between the two files in question, one reporting a psychiatric history of a certain seriousness, the other having the nature of a file of intelligence. Such a connection can only be envisaged with particular vigilance. It also recalls that insofar as certain information contained in HOPSYWEB is covered by medical secrecy, sufficient guarantees with regard to respect for the fundamental principles of the right to protection of personal data must be implemented. In this regard, the Commission considers that suitable legal and technical measures must be provided for in order to ensure a high level of data protection. On the new purpose of HOPSYWEB processing and the applicable legal regime: The Commission recalls that HOPSYWEB processing, on which it has already ruled, aim to ensure the follow-up of people undergoing psychiatric care without consent by allowing the administrative management of the associated measures. It indicates that this management is entrusted to the ARS within the framework of the departmental protocols established with the departmental prefects and, in Paris, with the prefect of police. However, the Commission notes that the draft decree aims to modify the purposes pursued by the HOPSYWEB processing by adding a new purpose of preventing radicalization. Indeed, Article 1 of Decree No. 2018-383 of May 23, 2018 is thus supplemented: the purpose of this processing of personal data is to monitor people undergoing psychiatric treatment without consent by allowing (…) the information of the representative of the State on the admission of people in psychiatric care without necessary consent

for the purposes of preventing radicalization, under the conditions provided for in book II of the third part of the code of public health referred to above and of the article 706-135 of the criminal procedure code. This new purpose results in an interconnection, provided for by the draft decree according to the methods described below, between the HOPSYWEB processing operations and the FSPRTIn the context in particular of the implementation of the national plan for radicalization, the ministry considers in fact that this information should enable the prefect of the department and, in Paris, the prefect of police, to know quickly and with certainty that a person being monitored for radicalization, including in another department, is the subject or has been hospitalized without consent in the departmental jurisdiction for which he is responsible in a context of high terrorist risk. The Commission observes that, in practice, the prefects will thus be able to identify people likely to present, due to a pre-existing psychiatric pathology which has given rise to a measure of hospitalization without consent, potential risks of harm to the safety of persons or to the public order. In this regard, the Ministry has indeed specified that if this information aims to improve the prevention of risks linked to the radicalization of people with psychiatric disorders by ensuring better monitoring of the latter, it must also allow them to decide on the appropriate actions to be taken with regard to the information already recorded in the FSPRT. Without calling into question the legitimacy of this new purpose, the Commission considers that the processing retains its main purpose of monitoring people undergoing psychiatric care without consent and that in this respect, the prevention of the risks linked to the radicalization of people with mental disorders is only a secondary purpose. The planned interconnection with the FSPRT does not have the effect of modifying the main characteristics pursued by HOPSYWEB processing, the general objective of which is to standardize and secure practices in terms of hospitalization without consent. The addition of the new purpose and the planned interconnection do not have the effect of bringing HOPSYWEB processing into the field of processing involving State security or defense within the meaning of the provisions of Article 26-I- 2° the law of 6 January 1978 as amended. HOPSYWEB processing also does not fall within the scope of Directive 2016/680 of April 27 referred to above. In view of the foregoing, the Commission considers that the conditions for implementing this processing must be examined with regard to of the provisions of the aforementioned GDPR. It recalls that, in accordance with Article 9-4 of the GDPR, specific provisions have been adopted in national law with regard to processing of health data. Under these conditions, the Commission recalls that it is also necessary to apply the provisions of the law of January 6, 1978. On the interconnection of HOPSYWEB processing with the FSPRT: The Commission notes that the addition of the new purpose of prevention of risks related to the radicalization of people with mental disorders implies that HOPSYWEB treatments

are interconnected with the FSPRT. In this respect, article 2 of the draft decree provides that for the purposes of informing the prefect of the department and, in Paris, the prefect of police, for the prevention of radicalization, the identification data (of HOPSYWEB processing ) referred to in 1° of Article 2 (surname, first names, domicile, sex, date and place of birth) may be linked to the identification data recorded in the automated processing of data at personal character referred to as FSPRT. The Commission notes that a cross-check between the data recorded in the two processing operations is carried out, at least every 24 hours. The FSPRT and HOPSYWEB processing operations are also queried, as soon as a new individual is registered in one of these two processing operations. The Commission also takes note of the clarifications provided that the cross-referencing of data will only be carried out using the surname, first name and date of birth of the person concerned. She asks that the draft decree be amended accordingly. It also notes that this interconnection will only relate to a strictly limited number of data, subject to phoneticization and hashing, and only relating to the surname, first name and date of birth of the person concerned. assumption of a match, i.e. if the person is known to the FSPRT and HOPSYWEB, the prefect of the hospitalization department can then take steps with the ARS to obtain additional information and ensure the identity of the person concerned as part of a procedure to clear up doubts. In this respect, the Commission notes that these exchanges taking place in this context are limited to what is strictly provided for by the provisions of the Public Health Code and the Code of Criminal Procedure, that is to say, in practice, the start and end dates of the measure, the type of measure taken and, where applicable, the place of hospitalization. Furthermore, it notes that the prefects will be informed that they must not, in the context of this removal of doubt, disclose the fact that the person concerned is registered in the FSPRT. The ministry has also indicated that the information communicated as part of the removal of doubt, will be via the usual transmission channels, for example by telephone. He specified in this regard that the ARS agents likely to respond to such requests are made aware of the confidential nature of the information transmitted. Finally, it was specified that the ARS is the prefect's privileged interlocutor within the framework of the CPRAF (unit for the prevention of radicalization and support for families), within which an identified referent from the ARS intervenes and may already be aware of cases of radicalisation. Although the Commission does not question the need for departmental prefects to verify the identity and collect additional information relating to the persons thus targeted through the intermediary of the ARS, it considers that in view of the particularly sensitive nature of the information in question (registration or not with the FSPRT), the procedures for exchanging the aforementioned information with the ARS, within the framework of the procedure for clearing up doubts, do not are not sufficiently supervised. In view of

these elements, the Commission wonders about the conditions under which the removal of doubts is brought to operate. It considers that only the referent identified within each ARS, intervening in the CPRAF, should verify the identity of the person and communicate additional information, at the request of the prefect of the department, and in Paris, of the prefect of police. It considers that such a measure would indeed be likely to limit the risks leading to the knowledge by ARS agents of the fact that a person is registered in the FSPRT at the time of the request from the prefect of the department, and to Paris, from the Prefect of Police. The Commission emphasizes that the change envisaged has no impact on the management of care measures without consent and on the primary purpose of HOPSYWEB. In the event of a match, only the prefect of the department of the place of hospitalization or the agents he designates will be informed of the said match via an email generated by the FSPRT. Furthermore, the Commission notes that the prefects and agents duly designated and authorized by the latter will not have access to HOPSYWEB and that users and recipients of HOPSYWEB processing will not be able to access the FSPRT. On data recipients: The draft decree provides that the recipients of the identification data of the persons concerned by a measure of hospitalization without consent and of additional information are the prefect of the department and, in Paris, the prefect of police of the place of hospitalization. The Commission takes note of the details provided by the ministry according to which, as part of the procedure for removing any doubts, the prefect of the department of the place of hospitalization can then contact, if necessary, the prefect of the department in charge of monitoring the radicalized person or the service in charge of this follow-up. In this regard, it was also specified that the competent prefect in charge of monitoring the radicalized person can also initiate a more in-depth assessment of the individual within the framework of the departmental assessment group (GED) or the CPRAF or even inform the FSPRT. Given these elements, the Commission considers that in practice it is possible to consider that both the prefect in charge of monitoring the radicalized person, the members of the GED and the CPRAF, or even the people accessing the FSPRT will be recipients of the information that a specific person is subject to a measure of hospitalization without consent. However, the Commission emphasizes that this draft decree, insofar as it allows access for these persons, who are not involved in the implementation of the measure of hospitalization without consent, to information that an individual is actually the subject of such a measure and to additional information in the event of implementation of the procedure for removing doubts (start and end dates of the measures, type of measure pronounced, where applicable place of hospitalization), raises questions with regard to the requirements of professional secrecy in this area. the occasion of an act of prevention, diagnosis or care are protected by professional secrecy, except in the cases of derogation

provided for by law. In the same way, it observes that the principle according to which only a legal derogation from the rule of professional secrecy authorizes a professional to access data covered by medical secrecy, is also recalled under the instructions of the months of January and December 2016 referred to above. .However, information relating to the care measures without consent to which a person has been subjected, in particular the additional information likely to be transmitted within the framework of the procedure for the removal of doubts, is likely to fall under the professional secrecy provided for in article L. 1110-4 of the public health code. Moreover, the Commission recalls that the information concerning the implementation of a measure of hospitalization without consent with regard to a specific person constitutes health data in accordance with the provisions of Article 4-15) of the GDPR, precisely in that it can reveal the nature of the condition (mental disorder) and provide, by itself, elements allowing its seriousness to be characterized. These elements recalled, the Commission has reservations about the possibility, for this draft decree, to introduce a derogation from professional secrecy which would allow, in particular agents accessing the FSPRT, to be recipients of information covered by medical secrecy. On the rights of individuals: The Commission notes that there are no plans to specifically inform the persons concerned, namely persons subject to a measure of hospitalization without consent, of the new purpose which would be pursued by the HOPSYWEB processing operations. However, the Commission recalls that such information is required under the provisions of Articles 12, 13 and 14 of the GDPR. Irrespective of the foregoing, the Commission considers that, given the evolution of the legal framework applicable to data protection at personal nature, it is up to the Ministry to ensure that the information currently issued by the ARS meets the requirements of the aforementioned provisions. In this respect, and given the challenges linked to the linking of HOPSYWEB and FSPRT processing, it considers that specific information, as to the new purpose pursued, should be issued. Furthermore, the Commission notes that the draft decree does not provide any provision on the right to erasure of information contained in HOPSYWEB, in particular when a care measure without consent is then declared irregular by the judge of freedoms and detention. In the same way, the Commission notes that the draft decree does not specify the procedures according to which the ARS concerned must notify the deletion of the data to the prefect of the department of the place of hospitalization in accordance with the provisions of Article 19 of the GDPR . While the Commission notes that the procedures for exercising the other rights remain unchanged, it nevertheless invites the Ministry to ensure that the rights mentioned are complete in order to take into account the contributions made by the GDPR. In particular, the Commission considers that the draft decree should be supplemented with regard to the implementation of the right to limitation of the

persons concerned. In the same way, it considers that the draft decree should be amended with regard in particular to the provisions applicable to the right of opposition and the reasons leading, in this case, to disregard it insofar as it is necessary to apply the provisions of Regulation (EU) 2016/679 referred to above. On data security: As a preliminary point, the Commission notes that HOPSYWEB processing is likely to generate high risks for the persons concerned within the meaning of Article 35 of the GDPR, an impact analysis was sent by the ministry. It stresses, however, that the absence of precise information on the architecture and the measures adopted does not allow the conformity of the device to be assessed with the security requirement provided for in Articles 5-1-f) and 32 of the GDPR. In general, it recalls that the nature of the data processed within HOPSYWEB processing requires that encryption measures in accordance with Appendix B1 of the general security reference system both at the level of databases and backups be implemented. logging of consultations, additions, modifications, deletions in HOPSYWEB processing, until now kept for 15 days, will be kept for one year. The Commission recommends, with regard to health data, that traces be kept in patient files and for a period equal to the retention period of these files. It also recommends that the administrator, who is able to consult the traces of access, does not access health data. Exchanges between the two systems HOPSYWEB and FSPRT are carried out via the HTTPS protocol. Regarding the use of this protocol, the Commission recommends using the most up-to-date version of TLS possible and using algorithms and key management procedures that comply with appendix B1 of the general security reference system. In addition, a mechanism for mutual authentication of the servers should be put in place. The method for verifying concordance between the two databases implements a cryptographic mechanism with a key. The Commission recalls the need to comply with the recommendations of the National Agency for the Security of Information Systems in this area and calls on the Ministry to be vigilant with regard to the means implemented for key management. Sensitivity of information calculated on each HOPSYWEB web service in the case of an addition in FSPRT requires that a security analysis of the device be carried out, including in particular intrusion tests and a code audit. The Commission recommends that the person(s) responsible for administering these services undergo specific training on the potential impact of this service on data subjects. Finally, a mechanism for logging any administrative action on this system should be implemented in such a way that these traces are not accessible to the aforementioned administrators. The Commission takes note of the ministry's commitment that no trace verification calculations will not appear on the system. It deduces from this that only traces of connections between the servers will be kept. In this context, and since a new connection between the webservices is made with each new entry into the FSPRT, the Commission notes that the

Ministry accepts the residual risk consisting in being able to deduce technical traces from any of the HOPSYWEB systems that a line has been added to the FSPRT, without knowing which one. As part of the procedure for removing doubts, the Commission stresses the need to implement a process allowing the authentication of the caller and the respondent before discuss any request. In addition, the risk that the person authorized to respond to this removal of doubt at the ARS deduces the reasons for the call is not negligible, measures to limit the seriousness should be put in place, for example by informing it of the high rate of false positives and by choosing a contact person authorized, moreover, to handle information of this type. The Commission also points out that the security requirement provided for by the articles5-1-f) and 32 of the GDPR requires the update of the impact analysis relating to data protection and its security measures with regard to the regular reassessment of the risks. In this respect, it underlines that the opening of the FSPRT to all the HOPSYWEB webservices implemented by each of the ARS has the effect of increasing the potential attack surface and requires that particular attention be paid to the choice of security measures. security carried out.The PresidentI. FALQUE-PIERROTIN