. ..... D

National Data Protection Commission

OPINION/2021/104

I. Order

1. The Secretary of State for the Presidency of the Council of Ministers asked the National Data Protection Commission (CNPD) to comment on the draft decree-law approving the structure of the National SIRENE Cabinet (hereinafter “Project”),

2. The CNPD issues an opinion within the scope of its attributions and powers as the national control authority for the processing of personal data, conferred by subparagraph c) of paragraph 1 of article 57 and paragraph 4 of article 36. of Regulation (EU) 2016/679, of 27 April - General Data Protection Regulation (RGPD), in conjunction with the provisions of article 3, paragraph 2 of article 4, and subparagraph a) of paragraph 1 of article 6, all of Law no. 58/2019, of 8 August, and with the provisions of paragraph 2 of article 30 and paragraph c) of paragraph 1 of article 44, both of Law No. 59/2019, of 8 August.

3. The SIRENE National Office1 is the entity responsible for exchanging supplementary information with its counterparts, within the scope of the alerts existing in the Schengen Information System (SIS), in accordance with Articles 7 and 8 of the SIS II Regulation2. and the SIS II Decision3.

4. The Project aims to approve a new structure of the National SIRENE Cabinet, revoking Decree-Law n.° 292/94, of 16 November, which created the National SIRENE Cabinet, and revoking paragraph 8 of article 21,° of Law No. 53/2008, of 29 August (Internal Security Law), which integrated the SIRENE Cabinet into the Security Coordinating Office (GCS), directly reporting to the Prime Minister, when before that it constituted an integrated organic unit in the National Schengen Information System (N.SIS), under the Ministry of Internal Affairs.

5. The Project now intends to remove the SIRENE Office from the scope of the GCS and integrate it into the Single Point of Contact for International Police Cooperation (PUC-CPI), which works under and under the coordination of the Secretary General of the Police System. Internal Security (cf. paragraph 3 of article 23-A of the Internal Security Law, in its current wording).

1 SIRENE is the acronym for Supplementary Information Request at the National Entries.

2 Regulation 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II Regulation).

3 Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II Decision).

Av.D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

II. Analysis

6. It should be noted first of all, as a preliminary matter, that the powers of the National SIRENE Office (hereinafter, «SIRENE Office»), as well as a set of rules and procedures to which it is subject, are currently provided for in the law of Union, insofar as the Schengen acquis has been integrated into the Treaties. Thus, there are specific legal instruments that regulate the functioning and use of the Schengen Information System (SIS), as well as the work of the SIRENE4 Office, and the Member States cannot legislate in violation of European standards in this matter.

7. In fact, although in some Schengen contexts there are references to national legislation, with regard to the functioning of the SIS, the Member States are conditioned to respect the limits imposed by EU law. This is particularly evident with regard to the objectives and purposes of the SIS, which is reflected in the processing of personal data in the SIS or in the scope of supplementary information, in the rights to consult the SIS by the different user entities and in the purposes of this direct access to the SIS, in the strict limitations on the use of SIS data for other purposes and on the prohibition of the transfer or availability of data to third countries or international organizations, or restrictions on the exercise of rights by data subjects.

8. To that extent, the CNPD will point out the rules of the Project in question that it considers to be violating the Schengen legal framework, as they go beyond the limits imposed by the legal instruments of the Union.

9. Secondly, given that the Union's current Schengen legal framework will be amended shortly, foreseeably in the first quarter of next year, when three new regulations that are already in force5 are fully implemented, the CNPD will naturally take into account takes into account, in its assessment, the novelties brought by these legal instruments.

i.Applicable national data protection regime

10. The Project refers, in some provisions, exclusively to the application of Law No. 59/2019, of 8 August, which approves the rules on the processing of personal data for the purposes of prevention, detection, investigation or prosecution of infringements criminal proceedings or enforcement of criminal sanctions, transposing Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.

4 See, in particular, in addition to the Convention Implementing the Schengen Agreement (CAAS), the SIS II Regulation, the SIS II Decision and the SIRENE Manual, which contain detailed operating rules for SIRENE bureaus.

5 Regulation (EU) 2018/1860, Regulation (EU) 2018/1861 and Regulation (EU) 2018/1862, all dated 28 November 2018, with the SIS II Regulation and the SIS II Decision being repealed.

CHklIFUIf^

O

National Data Protection Commission

11. Despite the SIS being a single system and functioning as such, the European Schengen legal regime is based on different legal bases: one relating to border control, asylum and immigration; the other on police and judicial cooperation in criminal matters.

12. This division has implications from the point of view of the processing of personal data, in particular, regarding the regime that applies to them, either to the data processed in the SIS, or to the data processed at national level to support the indications entered by Portugal or to the data processing carried out by the SIRENE Office, within the scope of the exchange of supplementary information and the verification of the quality of the data entered in the SIS by our country.

13. The personal data processed by the SIRENE Office therefore have two distinct legal frameworks that result from the different purposes pursued, with data processing that is not carried out for the purposes of prevention or criminal investigation.

In fact, the overwhelming majority of alerts on persons are made under Article 24 of the SIS II Regulation. However, in Chapter VI of that regulation, there are references to the application of Directive 95/46/EC (Data Protection Directive), which is understood to be made for the GDPR, pursuant to paragraph 2 of its article 94. °.

14. Therefore, the data processing carried out by the SIRENE Office applies at national level, in what is not specifically provided for in the EU legal instruments on Schengen6, both the GDPR and Law No. 58/2019, of 8 August, in relation to alerts in the SIS provided for in the SIS II Regulation, or Law No. 59/2019, of 8 August, in relation to alerts in the SIS provided for in the SIS II Decision.

15. The same will apply, in the near future, in relation to alerts in SIS provided for in Regulation (EU) 2018/1860 and in Regulation (EU) 2018/1861, which fall within the material scope of the GDPR, while alerts included under Regulation (EU) 2018/1862 fall within the scope of application of Directive (EU) 2016/680, which was transposed into the national legal order by Law No. 59/2019.

16. Therefore, the Project under analysis should be amended, in order to also include, as a national data protection regime applicable to data processing carried out by the SIRENE Office, the RGPD and Law No. 58/2019. Such an amendment must be made to Article 12, Article 14 and Article 16(2).

ii.Creation of referrals by Portugal

17. Decree-Law No. 292/94 currently grants the SIRENE Office the power to create, amend or delete Portugal's alerts in the SIS, upon instruction, request or delegation from judicial authorities and

6 As provided for in Article 31(9) of the SIS II Regulation, in Article 46(9) of the SIS II Decision, in Article 51(2) of Regulation (EU) 2018 /1861 and paragraphs 2 and 3 of article 66 of Regulation (EU) 2018/1862.

administrative tasks or at the request of security forces and services. It was an option of the Portuguese legislator at the time to centralize in a single entity the possibility of inserting, rectifying or deleting data in the SIS.

18. Not resulting from an imposition of Union law, this option has the advantage of allowing a uniform and consistent application of the criteria for the creation of alerts, with special emphasis on the verification of the legality of alerts. Precisely to control the legality and validation of acts that require its intervention, the law provides for the existence of a Public Prosecutor at the SIRENE Office, a rule that is maintained in this Project (cf. article 10), although no longer in functions only in the SIRENE Office, but in all the organizational units that make up the PUC-CPI.

19. In addition, the SIRENE Bureau is responsible for verifying the quality of data entered into the SIS (cf. Article 7(2), 3rd subparagraph, of the SIS II Regulation and the SIS II Decision), which it will certainly be much easier to reach if the SIRENE Bureau creates the alerts in the SIS.

20. In addition, the SIRENE bureaux have specific functions with regard to the compatibility of alerts and the affixing of references to alerts (cf. Articles 23 and 24 of the SIS II Decision), for which reason the National SIRENE bureau is responsible for creating , change and delete the indications, it is possible to more easily and rigorously ensure compliance with those legal requirements. In addition, in the new legal framework of the SIS, SIRENE bureaux are given expanded functions in terms of controlling the retention periods of alerts and deleting alerts after the expiry date (see paragraph 7 of article 39 of the Regulation (EU) 2018/1861 and Article 53(9) of Regulation (EU) 2018/1862).

21. It is not understandable, therefore, that the Project under analysis will now change the model centralized in the SIRENE Office to provide that any security force or service, any judicial and administrative authority, provided that it has the technical conditions for this purpose, can insert, modify, correct or delete the particulars (cf. Article 3(2)).

22. Extending the possibility of creating alerts in the SIS to several entities represents a dispersion of powers that certainly has consequences from the point of view of data protection, as it means granting access to the SIS with privileges to create, change and delete alerts to a wide set of entities, thus multiplying the risks of entering data without the proper quality, with disparate criteria, with less control of the principle of proportionality, in addition to enhancing the misuse of the system. This scenario would also make it difficult for the SIRENE Office to keep the supporting documentation for the alerts, in particular the references to the decisions that motivated the alert, as well as the control of the retention period of the alerts.

23. In this sense, it is the CNPD's understanding that a solution such as the one that currently exists of centralization in the SIRENE Office of the possibility of creating, altering and deleting indications is the one that best guarantees a higher level of compliance in terms of data protection7.

24. On the other hand, it will always be said that if it is the legislator's intention to open up this possibility, it will not be able to do so, in any case, under the terms set out in paragraph 2 of article 3 of the Project. In fact, it will have to be positively foreseen in law which entities are attributed that competence, identifying them and specifying which are the indications that they can insert, change and delete, and to determine if an indication introduced by entity X can be altered and/or eliminated by entity Y, in Portugal, and under what conditions it can do so.

25. In addition, as in terms of the technical architecture of the SIS and its operation, the data are entered in the SIS through the N.SIS, the extension of the possibility of creating alerts by entities other than the SIRENE Office should be made in special legislation on the N.SIS8 and not through the organic structure of the SIRENE Bureau (see Article 4(2) of the SIS II Regulation and the SIS II Decision).

26. The wording of paragraph 2 of article 3 of the Project has no legal support as it stands. In the understanding of the CNPD and for the reasons explained above, this function should, as far as possible, be centralized in the National SIRENE Office, as it currently stands.

27. This does not affect the possibility that, as is already the case today for certain types of indications, namely objects, the information is previously prepared upstream for a batch export, with the SIRENE operator always being responsible for validating those indications and the effective creation of indications. It is in the light of this scenario, moreover, that the function provided for in subparagraph g) of paragraph 1 of article 3 of the Project is understood. In this way, the SIRENE Office maintains the necessary control over alerts, including to fulfill the duties legally conferred on it by Union law.

iii. Connection to other SIRENE offices

28. In paragraph 3 of article 4 of the Project, it is foreseen that the SIRENE Office will guarantee the link with the other similar offices and ensure the exchange of complementary information (...) through the PUC-CPI operational center .

1 Account should be taken of the experiences of other Member States, as shown in the Schengen evaluation reports with a negative assessment, revealing the problems arising from having several entities entering data in the SIS.

8 Under the law, the person responsible for processing N.SIS data is the Aliens and Borders Service.

Av.D. Carlos 1,134.1°

1200-651 Lisbon

T(+351) 213 928400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

29. Firstly, it is suggested that the term “additional” be replaced by “supplementary”, for the sake of consistency with the terminology used in the legal instruments and which is explicitly defined in Article 3 of the SIS II Regulation and the SIS II Decision.

30. Secondly, the scope of this rule is not understood in connection with the other SIRENE bureaus. In this Project, it is foreseen that the SIRENE Office will become part of the PUC-CPI, justifying this option in the preamble of the Project, as there is a functional identity between SIRENE and the PUC-CPI, namely due to its uninterrupted operation and the possibility of to achieve synergies and optimize human resources by sharing support services and information technologies. However, the link between SIRENE bureaux for the exchange of supplementary information is already legally established in Article 4 of the SIS II Regulation and the SIS II Decision, which establishes the architecture and functioning of the SIS.

31. It states that the connection between SIRENE offices is made through the communication infrastructure between the CS-SIS technical support function and the NI-SIS national interface (cf. Article 4(1)(c)). of the Union legal instruments listed above). This means that the connection must be made point-to-point without any intermediate connection channel, nor the communications between the National SIRENE Office and its counterparts must be in any way intermediated by other actors, guaranteeing the complete segregation of traffic. , regardless of organic and functional dependencies.

32. In addition, if there is a possible intermediation of the connection between SIRENE offices through a channel, network or

PUC-CPI system (operational centre), there would be the possibility of accessing, copying and preserving the content of communications and personal data contained therein, the which would represent an additional processing of personal data, without any basis of legitimacy.

33. This is precisely one of the matters in which the Portuguese legislature cannot contravene the provisions of EU law. In this way, paragraph 3 of article 4 of the Project must be amended to bring it into line with the European Schengen legal instruments, or else clarified what exactly is intended to regulate in this rule.

iv. Access to national databases by SIRENE operators

34. Article 7 of the Project provides that the operational service of the SIRENE Office will be provided by elements of the GNR, PSP, PJ and SEF, reflecting what is already happening in practice today. It determines their main skills and requires them to have appropriate qualifications for their exercise.

35. In paragraph 4 of that article, it is established that SIRENE operators have direct access to all information, including national databases and information systems, and to all information on alerts introduced by Portugal, according to the principle of the need to know.

36. It would not be possible to be more open and comprehensive in this rule, contrary to the principle of need to know, and there is not even any justification for this purpose in the preamble of the Project regarding the need to access any database or information system national law, which would be a prerogative without precedent in national law.

37. Naturally, a legal provision of this nature, when it comes to access to personal data and, therefore, an interference with fundamental rights, does not have the necessary degree of precision or the safeguards inherent to this level of compression of rights, thus achieving the predictability of its effects, so it does not allow the assessment of its suitability, necessity and proportionality in the strict sense, not complying with the principle of proportionality in the broadest sense, according to the consolidated jurisprudence of the Court of Justice of the European Union (CJEU) and of the European Court of Human Rights (ECtHR).

38. This proposed legal provision identifies two types of direct access: one relating to information related to alerts in the SIS introduced by Portugal, and another, more general, to all national databases and information systems.

39. As for information related to Portuguese alerts, this is necessary in the context of the exchange of supplementary information, and part of this information must already appear in the documentation held by the SIRENE Office, in support of the alerts created by Portugal, associated with requests creation of such alerts and to enable the necessary data to be entered in the SIS, including the reference to the decision that gave rise to the alert, which constitutes a mandatory entry data when creating an alert under the SIS II Regulation and, in some cases, also under the SIS II Decision (cf. Article 23 of the SIS II Regulation and the SIS II Decision).

40. Thus, in addition to the information that must already be in the possession of the SIRENE Office, there may still be a need to consult additional information. This is guaranteed through the access that each SIRENE operator has to the information systems of the security force or service from which it comes, thus ensuring that the systems of the GNR, PSP, PJ and SEF can be consulted, if necessary.

41. However, given the 24/7 operation of the Office and the existence of shifts, immediate access to all these systems may not be guaranteed {e.g., during the night, when, as a general rule, the presence of 4 elements, one from each entity).

42. In accordance with the rules defined for the functioning of the SIRENE Bureaux in the new SIS regulations, requests for information must be answered as soon as possible and no later than 12 hours after their receipt9. This period will thus make it possible to overcome the constraints that may exist when elements of all the forces represented in the operative service are not present.

43. But even assuming that, in order to deal with emergency situations, also provided for in the European legal framework of the SIS, requiring immediate action, it is necessary to find a solution that allows access by all SIRENE operators to the information systems of all forces that make up the operative service, such a possibility would have to be duly established by law, with well-defined objectives, its exceptional nature and provision for technical safeguard measures that effectively limit

these accesses to what is strictly necessary and justified (for example , through a specific access profile for this purpose, provided by each of the entities responsible for the systems, with a "break-the-glass" solution accompanied by the justification of access, in order to allow its monitoring and auditability).

44. As for the other, even more general type of access to any and all databases or information systems, for added reasons, it would not be admissible for the reasons set out in points 36 and 37 of this opinion. If there are specific needs for the SIRENE Office to have access to other databases, in addition to those that each operator already has within the scope of legally authorized access for its security force or service (e.g., civil identification database, databases of data from public records, criminal records) - and, to that extent, access is already guaranteed - this should be provided for by law with the identification of the information systems in question, justifying the need for access and its limits, as well as foreseeing the appropriate safeguard measures.

45. In short, the wording of paragraph 4 of article 7 of the Project violates the Constitution of the Portuguese Republic and the national data protection regime, and this provision should be deleted, due to its obvious disproportionate, but also because this matter is in the legislative reserve of the Assembly of the Republic, and cannot be innovatively regulated in this decree-law (cf. paragraphs 2 and 3 of article 18 and paragraph b) of paragraph 1 of article 165 of the CRP).

9 See Article 8(3) of Regulation (EU) 2018/1861 and Regulation (EU) 2018/1862.

v. Entities that use the SIS

46. The Project establishes, in article 5, a non-exhaustive list (via the expression "namely") of entities using the SIS, that is, with the right to consult the data contained therein, to be indicated by the Portuguese State10, upon communication from the Secretary General of the Internal Security System.

47. As a first observation, the CNPD points out that the list of entities with rights of direct access to the SIS for consultation purposes falls within the scope of the functioning of the N.SIS, insofar as access is made through the national Schengen system, being responsible for the treatment responsible for ensuring the security of the system, managing user profiles and

monitoring access. In this sense, from the point of view of legislative systematization, it would be preferable for the designation of the competent authorities to consult the SIS to be carried out in autonomous legislation and not within the framework of the organic structure of the SIRENE Office, which is also a user of the SIS by virtue of its attributions conferred by the European Schengen legal instruments.

48. Second, there is no basis in the powers legally assigned to the SG-SSI11 for it to decide which national entities can have direct access to the SIS for consultation purposes, in addition to those that are now proposed in this Project. Furthermore, this is not even a relevant issue in terms of the structure of the SIRENE Office, insofar as the consultation of the SIS by other entities does not represent any interference in the activity of the SIRENE Office. Access by the SIRENE Office is already legally provided for in the European legal instruments that regulate the functioning of the SIS, and therefore does not require a national legal provision.

49. Therefore, in order to maintain the list of entities that use the SIS in this Project, that is, with privileges to consult the SIS directly - which will always be preferable to not being clearly identified in national law -, this matter must be object of another systematic arrangement in this decree-law, more differentiated from the functioning of the SIRENE Cabinet, which is effectively unrelated.

50. On the other hand, the rule must be revised, in the sense of removing the expression “namely” so that the list of legally foreseen entities is closed. law, that it is not up to the SG-SSI to communicate this listing to the SIS managing authority, as provided for in the Schengen legal instruments, but perhaps to the person responsible for the N.SIS.

10 This is presumed to be the indication to the European agency eu-LISA, as the managing authority of the SIS, of the competent national authorities authorized to consult the SIS directly, as referred to in Article 46(8). of the SIS II Decision and Article 31(8) of the SIS II Regulation.

11 Provided in Articles 16 to 19 of the Internal Security Law.

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

51. Once the list of SIS user entities is established, the Project must specifically add which Schengen indications to which each of them has the right of access, taking into account their legal attributions and the purposes of access, in accordance with the limitations established in the articles 34 and 41 of Regulation (EU) 2018/1861 and in articles 44 to 47 of Regulation (EU) 2018/1862.

52. The CNPD believes that, since the three new Schengen regulations have brought about an extension of the purposes of consulting the SIS (e.g., for the purpose of naturalization of foreigners and for the purpose of issuing registration certificates for vessels and aircraft), implying an increase in the number of competent authorities with access to the SIS, the Project should already foresee the list of national entities that will be users in the near future.

53. Now, with regard to the entities listed in paragraph 1 of article 5 of the Project, it would be said that the entities provided for in subparagraphs a) to j) all meet the criteria defined in the new European legal instruments of the SIS12, with the exception of the National Civil Aviation Authority (ANAC), these entities already have the right of access to the SIS, although not all do so in practice.

54. However, a novelty is introduced in this Project, in subparagraph k) of paragraph 1 of article 5, in which it is intended to give direct access to the SIS to the operational center and other organizational units of the PUC-CPI. Also in this matter, the preamble of the Project does not reveal anything about the underlying reasons for this concession.

55. In the opinion of the CNPD, there is no legal basis for making the PUC-CPI, through its organizational units, an entity that uses the SIS, and such access cannot be carried out without violating Union law on Schengen matters, and eventually national law. If not, let's see.

56. Pursuant to paragraph 1 of article 23,°-A of the Internal Security Law13, the PUC-CPI is the operational center responsible for coordinating international police cooperation, which ensures the forwarding of national requests for information, the reception , the forwarding and national dissemination of information from foreign police authorities, the transmission of information and the fulfillment of requests made by them.

57. For this purpose, the PUC-CPI is made up of five organizational units, brought together under the same management and

coordination, namely, in addition to the SIRENE Office: the EUROPOL and INTERPOL Office, the Office for Police and Customs Cooperation Centers (CCPA), the newly created Passenger Information Office and the Office for National and Foreign Liaison Officers and Prum Decisions Contact Points (cf. paragraph 4 of article 2 of Decree-Law no. 10/2020, of March 11, which establishes the structure of PUC-CPI).

12 Without prejudice to the verification of the adequacy of access to specific indications.

13 In the wording given by Decree-Law No. 49/2017, of 24 May, which created the PUC-CPI.

58. In fact, the PUC-CPI is what its name implies and no more than that, in the sense of facilitating international police cooperation, in the legally prescribed terms, through a certain centralization of the exchange of police information, whether both at European Union and international level, without prejudice, of course, to the conditions imposed by the specific legal instruments of the Union that regulate such police cooperation, as well as the constraints provided for in special national legislation.

59. Thus, regardless of the possible functional coordination, convergence of action and optimization of human resources and support services, the integration in the PUC-CPI of different offices, created in different legislative contexts and with different objectives, does not mean that the legal attributions of each are confused or that can be collectively shared, as intended here.

60. Among the purposes set out in the SIS regulations that support the consultation of the SIS by competent authorities, international cooperation is not provided for in itself. Schengen has its own well-regulated cooperation mechanisms. The PUC-CPI is essentially a facilitator of information exchange at various levels, not carrying out, in itself, police checks within the national territory or carrying out criminal investigations. Nor is it a competent entity for the pursuit of any other purpose provided for in the SIS regulations, which may allow direct access to the SIS.

61. Furthermore, the European Schengen legal regime in force limits the processing of SIS data, including access, to the legally foreseen purposes and within the limits of the powers of the entities authorized to access, considering any action outside this framework to be abusive. legal14.

62. On the other hand, there is a strict prohibition on transferring personal data from the SIS to a third country or international organization or otherwise making such data available. This is a historic norm in the Schengen legal regime and which is maintained in the new regulations15. The SIS has the general objective of guaranteeing a high level of security in the territories of the Member States and cannot be put at the service of any State that is not a Party to Schengen. Hence, outside the Schengen cooperation framework, SIS data cannot be used in the context of another type of international cooperation, which further removes the possibility of giving direct access to the SIS to all organizational units of the PUC-CPI , including third country liaison officers.

14 See Articles 31 and 46, respectively, of the SIS II Regulation and the SIS II Decision, as well as Article 41(7) of Regulation (EU) 2018/1861 and No. 6 of Article 56 of Regulation (EU) 2018/1862.

15 In accordance with Article 39 of the SIS II Regulation, Article 54 of the SIS II Decision, Article 50 of Regulation (EU) 2018/1861 and Article 65 of Regulation (EU)) 2018/1862.

Av.D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

63. For all these reasons, the PUC-CPI does not meet the legal conditions, both at the national level and in the European legal framework relating to Schengen, to be indicated as an entity authorized to directly access the SIS and consult the data processed there. To that extent, the provision contained in subparagraph k) of paragraph 1 of article 5 of the Project must be eliminated.

vi. Data protection officer, security incidents and terminology

64. In relation to article 16 of the Project on the Data Protection Officer (DPO), in addition to the observation regarding paragraph 2 made in point 15 of this opinion, it is recommended that it be explained in paragraph 1 or in an autonomous

number that the EPD reports to the Coordinator of the SIRENE Office, taking into account the form of formal appointment, in case it is impossible for the Coordinator to carry out the appointment directly.

65. In addition, Article 16(1) should still be amended, in order to adapt the EPD's functions to the legally required, since the EPD's role is not to replace the controller in the compliance with its legal obligations. Thus, it should be clarified that the EPD assists the controller in complying with legal obligations in terms of data protection16.

66. With regard to paragraph 4 of article 13 of the Project, on the notification of personal data breaches, this rule should be deleted, since there is already a specific rule in the new SIS regulations on which legislation is applicable to these security incidents, being the RGPD and Directive (EU) 2016/680, transposed into national law by Law n.° 59/2019, of 8 August.

67. Finally, some rules are highlighted that require, in terms of terminology, alignment with the current legal framework in terms of data protection and, specifically, within the scope of the SIS. Therefore, the heading of Article 15 of the Draft should be changed to “data controller” instead of data protection officer.

68. In the references that are made to the rights of data subjects (in Article 3(1)(i) and in Article 6(2)(h), the wording must be changed to specifically reflect the rights in question that can be exercised by persons who may not be targeted by the alerts. Thus, it should be made clear that this is about the rights of access, rectification and erasure of data by natural persons in relation to personal data processed in the SIS.

16 In accordance with the framework of functions provided for in Article 39 of the GDPR, in Article 11 of Law No. 58/2019, of 8 August, and in Article 35 of Law No. 59/2019 , of the 8th of August.

III. Conclusion

69. The national legal data protection regime applicable to the processing of personal data carried out by the SIRENE Office must be extended to the RGPD and to Law No. 58/2019, of 8 August, under the terms mentioned in point 16 of this opinion.

70. If opting to extend the possibility of creating, changing and deleting alerts in the SIS to several entities, such competence must be legally foreseen for each entity, duly identified, determining which SIS alerts each one can create and under what conditions. It is recommended, in any case, to centralize this attribution in the National SIRENE Office, given the other

attributions it has in the management of alerts, in the control of the quality of the data and, in the near future, in the control of the retention periods of the indications, striving to if so by the deletion of paragraph 2 of article 3 of the Project.

71. Article 4(3) of the Project should be amended in order to clarify what precisely is being regulated, given that the connection between SIRENE Bureaux for the exchange of supplementary information must be made in accordance with defined in the technical architecture of the SIS by Union law, that is, through the SIS communication infrastructure, with absolute traffic segregation, thus not admitting any type of intermediation in these communications.

72. The provision in paragraph 4 of article 7 of the Project, which generically provides for indiscriminate access, without justification of its need, without any type of limits and without safeguards, to any national information system by the SIRENE operators, violates the Constitution of the Portuguese Republic and the data protection regime, and should therefore be deleted. As it is a question of legislating on access to processing of personal data by third parties, this cannot be done within the scope of this decree-law, as it is a matter of the relative reserve of legislative competence of the Assembly of the Republic, in addition to meeting the legal requirements indicated in the points 43 and 44 of this opinion.

73. The list of entities using the SIS, that is, with access rights to the SIS for consultation, must be an exhaustive list and not just indicative or illustrative, and it must be expressly defined in the legislative text to which indications of the SIS can access and for what purposes. The provision contained in subparagraph k) of paragraph 1 of article 5 of the Project, which makes the PUC-CPI as a whole as a user entity of the SIS, should also be eliminated, as it clearly violates the access limitations provided for in the regime. European legal framework for the SIS as well as national legislation.

74. Article 13(4) of the Draft should be deleted as the way in which security incidents are reported is already regulated in Union law.

Av.D. Carlos 1,134.1st

1200-651 Lisbon

I (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

75. Minor changes should be made to Articles 3, 6 and 15 of the Draft, for the sake of precision, to reflect the terminology of the applicable legal regime, as indicated in paragraphs 67 and 68 of this opinion.

Lisbon, August 16, 2021

Filipa Calvão (President, who reported)