□AVG/2021/401

1

^NPD

National Data Protection Commission

DELIBERATION/2022/1072

f

I. Report

1.The National Data Protection Commission (hereinafter "CNPD") prepared the Draft Deliberation/2021/22, on October 19, 2021, in which the National Institute of Statistics, I.P. (hereinafter "INE"), the practice, in material authorship and in the consummated form, of ten administrative offenses arising from the violation of various provisions of Regulation (EU) 2016/679, of April 27 - General Regulation on Data Protection (hereinafter "INE") "RGPD"), referring to personal data processing activities carried out in the context of the "2021 Census" census operation, namely:

The. An offense provided for and punished by the combined provisions of Article 5(2) and Article 83(5)(a), both of the RGPD, with a fine of up to €20,000,000 or up to 4% of the annual turnover, for breach of the liability principle;

B. An offense provided for and punished by the combined provisions of Article 5(1)(a) and Article 83(5)(a), both of the RGPD, with a fine of up to €20,000,000 or up to 4% of annual turnover, for violating the principle of lawfulness, loyalty and transparency;

w. An offense provided for and punished by the combined provisions of Article 9(1) and Article 83(5)(a), both of the RGPD, with a fine of up to €20,000,000 or up to 4% of the annual turnover, due to violation of the prohibition on processing special categories of personal data;

d. An offense provided for and punished by the combined provisions of paragraph c) of paragraph 1 of article 5 and paragraph a) of paragraph 5 of article 83, both of the RGPD, with a fine of up to €20,000,000 or up to 4% of annual turnover, due to violation of the principle of minimization;

It is. An offense provided for and punished by the combined provisions of Article 32(1) and Article 83(4)(a), both of the RGPD, with a fine of up to €10,000,000 or up to 2% of the annual turnover, due to violation of the application of personal data security measures;

f. An offense provided for and punished by the combined provisions of Articles 12 and 13 and Article 83(5)(b), both of the RGPD, with a fine of up to €20,000,000 or up to 4% of the volume annual business, for violation of the duties of informing data subjects;

g. An offense provided for and punished by the combined provisions of paragraphs 1, 6 and 7 of article 28 and of paragraph aj of paragraph 4 of article 83, both of the RGPD, with a fine of up to €10,000,000 or up to 2% of

Av. D. Carlos 1,134,10

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

r

annual turnover, due to breach of compliance with the rules applicable to contracting subcontracting entities;

H. An offense provided for and punished by the combined provisions of Article 44, Article 46(2) and Article 83(5)(c), both of the RGPD, with a fine of up to 20,000,000 € or up to 4% of the annual turnover, for violation of the transfer regime;

i. An offense provided for and punished by the combined provisions of paragraphs 1 and 2 and paragraph b) of paragraph 3, all of article 35, and paragraph a) of paragraph 4 of article 83, all GDPR, with a fine of up to €20,000,000 or up to 4% of annual turnover, for breach of carrying out an impact assessment on the protection of personal data;

j. An offense provided for and punished by the combined provisions of Article 37(7) and Article 83(4)(a), both of the RGPD, with a fine of up to €20,000,000 or up to 4% of the annual turnover, due to breach of the duty to communicate, to the Control Authority, the designation of the Data Protection Officer (hereinafter "DPO").

2. The Defendant was notified of the content of the aforementioned Draft Deliberation and invited, if he wished, to present a defense [cf. Article 50 of Decree-Law No. 433/82, of October 27 (General Regime of Administrative Offenses and Fines, hereinafter "RGCO")].

3. The Defendant, in this sequence, alleges, in short, that:

i. The CNPD does not have the power to syndicate INE, because its powers have to be exercised exante within the organic-institutional framework of the Higher Statistics Council;

ii. The Deliberation Project is void due to the lack of representation of the assumptions of attribution to the Defendant of the committed infractions;

iii. The Draft Resolution is inadmissible for lack of prior notice, pursuant to the provisions of article 39(3) of Law No. 58/2019, of August 8;

iv. The Deliberation Project violates the technical independence of the Defendant and as such must be declared void;

v. The Defendant cannot be punished twice for committing the same act;

saw. The data processing was lawful;

vii. The Defendant did not violate the principle of minimization, in operations considered to be optional;

viii. The Defendant complied with the duties of informing the holders of personal data;

ix. The Defendant did not violate the duties of due diligence in choosing its subcontractor;

x. There was no transfer of data to third States, so the Defendant did not violate the data transfer regime;

xi. The Defendant was not obliged to carry out an Impact Assessment on Personal Data, since the assessment would have already been carried out in Authorization No. 2600/2011, issued by the CNPD, which was not subject to any amendment;

xii. The EPD contacts were communicated to the Control Authority, on May 22, 2018;

xiii. The Defendant requests waiver of the fine, pursuant to Article 44, paragraph 2, of Law No. 58/2019 of August 8.

4. As the CNPD detected that the copy of the file sent via email on January 24, 2022 did not contain the evidence collected and attached to information 2021/109, of September 16, 2021, the same were sent by dispatch of September 15, 2022, granting a new deadline for defense.

5. On September 29, 2022, the agent responded by informing that she maintained her previous defense.

II. appreciation

6. The CNPD is competent pursuant to paragraph a) of paragraph 1 of article 57 and paragraph 2 of article 58 of Regulation (EU) 2016/679, of 27 April 2016 - Regulation General Data Protection Regulation (GDPR), in conjunction with article 3, paragraph 2 of article 4, and paragraph b) of paragraph 1 of article 6, all of Law no. ° 58/2019, of August 8 (LERGPD).

7. It should also be said that, in everything that is not provided for in the LERGPD, the RGCO is subsidiarily applicable (by virtue of the provisions of Article 45 of that law).

8. In view of the Defense presented by the Defendant, it is necessary to assess the factual and legal arguments set out therein.

Like this:

Av. D. Carlos 1,134,10

1200-651 Lisbon

T(+351) 213 928400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

i. On the incompetence of the CNPD to syndicate the INE

9. The Defendant begins by alleging, in points 7 to 16 of his Defence, an argument that he later develops in points 39 to 148, that the CNPD "[...] had the opportunity to exercise its powers of ex ante control, within a framework organic-institutional structure specifically conformed with the purpose of integrating the contributions of the CNPD regarding matters relating to the processing of personal data in the context of the census operation, “but chose to act outside the institutional framework for the established effect and contrary to the resolutions adopted by the bodies in which it is integrated - and to which it should be considered linked -, attributing ex post the commission of a set of infractions that - having been verified, which is not granted -, the CNPD itself should unofficially have contributed to anticipate and prevent. " (points 14 and 15 of the Defense).

10. It is important, first of all, to clarify the misunderstanding in which the Defendant is working, perhaps the result of his poor understanding of the legal regime for the protection of personal data to which he is subject.

11. The legally foreseen participation of the CNPD within the Higher Statistics Council (CSE) is limited to the competences of

this body, which are foreseen in article 13 of the Law on the National Statistical System (Law no. 22/ 2008, May 13). The Defendant highlights, in point 43 of his Defence, two of these competences, although incompletely, thus distorting their real scope, which is why the full wording of these two competences is left here: "Define and approve the general lines of statistical activity officer and respective priorities;" "Formulate recommendations within the scope of defining methodologies, concepts and statistical nomenclatures for the use of administrative acts for the production of official statistics and to ensure their application".

12. However, an interpretation of that legal diploma that leads to the conclusion that, regarding the processing of personal data carried out by INE within the scope of the entity's statistical activity, the CNPD must exercise the powers conferred by the RGPD and the LERGPD only within the Council Superior de Statistics, would mean the exclusion of those treatments from the powers of successive and corrective supervision that the RGPD explicitly attributes to any national supervisory authority - cf. paragraphs 1 and 2 of article 58 of the RGPD exclusion that the national legislator did not provide for and which, moreover, would not be admissible in the national legal order in the face of European Union law.

13. What the Defendant persists in ignoring is that the function of the CNPD is, since the application of the new data protection legal regime began, essentially of supervision or successive control of the processing of personal data, focusing on prior control in general guidelines regarding the processing of personal data.

14. It is true that the CNPD has some competences in terms of concrete prior control (listed in paragraph 3 of article 58 of the RGPD), but the essential part of these competences presupposes the initiative of the controller, upon presentation of application to the CNPD, in accordance with the principle of proactive responsibility (accountability) enshrined in Article 5(2) and Article 24 of the RGPD.

15. In any case, within the scope of meetings of the CSE and its sections, the function of the CNPD is not, strictly speaking, that of supervision or prior control of the processing of personal data carried out by INE, but only that of contributing with its specialized knowledge and experience in the application of the principles and rules of protection of personal data for the definition of the general lines of the statistical activity, as well as methodologies, concepts and statistical nomenclatures for the use of administrative acts for the production of official statistics. In particular, within that body, the CNPD contributed to the

establishment between INE and the relevant public entities of a procedure for accessing data on citizens that would speed up the 2021 census operation and mitigate the impact on the rights of data subjects, promoting the pseudonymization of the data, a contribution that, after all, was not used.

16. For this reason and also because neither the RGPD nor the national and European legislation on statistical activity remove the personal data protection regime from statistical operations - rectius, because this legislation expressly safeguards the personal data protection regime -, maintain -the powers of the CNPD remain untouched, whether in the context of prior control or in the context of successive supervision, maximum those of inspection and sanctions.

17. Furthermore, and contrary to what the Defendant seems to intend, there is no contradiction between the different contributions of the CNPD within the CSE or its sections and the draft deliberation, since the CNDP at no point in the draft questioned or censored the variables defined by INE, as well as the option of collecting data via the Internet. In fact, the consistency of the CNPD is evident, taking into account that, within the Eventual Section for Monitoring the 2021 Censuses (SEAC), it warned of the specific risks arising from the online collection of responses to surveys.

18. What the CNPD found and is analyzing is not whether the variables are necessary for the census activity - given that the judgment of need was explicitly attributed to INE by national law and that the name of the respondents is not a variable, as it is clear from the Annex to Regulation (EC) 1201/2009, of November 30, 20091-, neither is the methodology and procedure for collecting these data; what the CNPD has ascertained and is analyzing are the legally defined conditions and limits for the processing of

1 Available at https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32009R1201 &from=PT

Av.D. Charles 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

personal data, in particular respect for the principles of lawfulness of processing and minimization of data and risks to the rights of data subjects, which include, for example, questions related to the identification of respondents and their family members (full name) and the pseudonymization of the data.

19. And the investigation and eventual sanction of the disrespect for such conditions and limits fall within the attributions and competences of the CNPD, as it follows from articles 55 and 58 of the RGPD and articles 3 and 6 of the LERGPD, therefore, the allegation in points 7 to 16 and 39 to 148 of the Defense does not deserve merit.

20. Furthermore, in previous census operations, although the CNPD was already a member of the CSE, INE never had doubts about the need to request the then necessary authorizations for the processing of data, nor did it question the role of the CNPD for inspection within the scope of these operations2 . In other words, despite the CNPD's participation in the CSE, INE has always considered that the CNPD's intervention as a national data protection authority did not end with its participation in that body.

21. In short, the collegial decisions of the CSE, in which the CNPD is one of more than twenty members, cannot condition the role of supervisory authority regarding the processing of personal data, under penalty of emptying its power recognized by the RGPD and by national law.

22. It is also important to clarify that the definition of concrete technical and organizational measures that will be applied in the census operation with reflection on the processing of personal data does not fall within the powers of the CSE, nor has it ever been raised in it.

ii. The lack of representation of the attribution assumptions

23. The Defendant alleges that, in the Draft Decision, there is no indication of the facts of the offense, based on the provisions of article 50 of the RGCO, paragraph 10 of article 32 of the Constitution of the Portuguese Republic (hereinafter "CRP") and articles 120, paragraph 1, paragraph 2, paragraph d), and paragraph 3, paragraph c), of the Code of Criminal Procedure, applicable by reference to the provisions of article 41. ° of the RGCO.

24. The Defendant considers, in the Defense presented, that the Draft Deliberation is silent as to relevant elements for the imputation of the infractions, with only a generic indication of the administrative offenses that are imputed to him.

2 See, for example, Authorization No. 2600/2011, of March 24, regarding the 2011 census operation and Deliberation No. 144/2012, of February 27, 2012, regarding inspection compliance with the conditions imposed in that authorization.

25. In the Defendant's understanding, the Draft Deliberation should include the motivation for acting, the circumstances in which the infraction was committed and the title to which the Accused was charged (intent or negligence).

26. In short, the Defendant understands that the Draft Deliberation does not contain the objective and subjective elements that allow him to be charged with committing an administrative offence.

27. As a result, he alleges that he is unable to exercise his right to a full and effective defense, which, in his opinion, should lead to the nullity of the present administrative offense proceeding, after the delivery of the Draft Deliberation.

28. Such an understanding is not acceptable.

Let's see,

29. Contrary to what the Defendant argues, the Draft Deliberation did not omit any elements that should have been included therein, the objective facts integrating the offense being clearly identified. It is further noted that, in the Draft Decision, reference is made to the facts that reflect the subjective imputation and those that may have influence in the concrete determination of the sanction to be applied.

30. It should also be recalled that a Draft Deliberation does not correspond to a final decision, so the presentation of grounds can - and should, for simplification of the process - be done succinctly.

31. Now, evaluating the Defense presented, it is easily verified that the Defendant knows all the foundations of the proposed decision, being undeniable that he is aware of the cognitive and evaluative iter of the decision, and of all the context that is applicable to him.

32. Pursuant to Decision No. 1/2003, of the Supreme Court of Justice, the administrative authority is not required to in the "accusation" (or, as the law determines, in the "counterordination that [...] is imputed" to the defendant) an evaluation of the evidence is carried out from the outset.

33. In other words, it is not required that the administrative authority, right in the "accusation", has to qualify the specific degree of seriousness or degree of guilt of the agent.

34. What is required is that, depending on the facts established and imputed to the defendant, the legal classification of the infraction, that is, the administrative offence, identify the corresponding applicable legal type (principle of typicality).

35. For example, if a rule establishes that a certain offense is punishable by way of malice, the "accusation" must contain the integrative facts of this legal type (the facts imputed to the defendant must

Av. D. Carlos 1,134,10 T (+351) 213 928 400 geral@cnpd.pt

1200-551 Lisboa F (+351) 213 976 832 www.cnpd.pt

allow extracting this legal misdemeanor qualification). The determination of the degree of seriousness of the infraction - and, therefore, of the agent's degree of guilt - will have to result from a specific judgment of evaluation of the evidence to be made in the instructional phase3.

36.Now, in the Draft Resolution it is clearly defined under what subjective title the infractions are imputed to the agent, either by identifying the elements that frame it

37. See, namely, points 129,130,131, where it is expressly stated that "the defendant did not act with the care to which he was bound and of which he was capable, representing as possible that he was acting against the law", description corresponding to attribution by way of negligence and points 132, 133 and 134, where it is expressed that "configuring an action that fits in the modality of possible fraud".

38. In these terms, the argument that the Draft Resolution is tainted by any procedural defect is rejected.

iii. The obligation of prior warning of the Defendant

39. The Defendant alleges that Article 39(3) of the LERGPD enshrines an obligation for the supervisory authority to give prior warning before initiating an administrative offence.

40. In the understanding, postulated in the written Defense, the Defendant considers that such prior warning is a procedural assumption or a condition of proceeding.

41. Failure to verify the aforementioned prior warning, according to the Defendant, entails the legal inadmissibility of the administrative offense proceeding.

42. The Defendant concluded that the Draft Deliberation should be declared null and void, due to violation of the principle of

legality.

Let's see,

43. Article 39(3) of the LERGPD establishes that "(...) [except in the case of fraud, the initiation of an administrative offense proceeding depends on prior warning of the agent, by the CNPD, in order to comply with the omitted obligation or reinstatement of the violation violated within a reasonable time (...)".

44. First of all, this provision would always be excluded in situations where there are intentional infringements committed by the controller, as is the case with some of the infringements in question.

3 In Administrative Offenses in Administrative Courts, CEJ E-Book, October 2019, p.113.

w

.... __ National Data Protection Commission

45. In any case, with regard to infringements imputed by way of negligence, that legal provision makes prior warning dependent on the possibility of "(...) compliance with the omitted obligation or reinstatement of the violation violated within a reasonable period

46. The violations that support the present administrative offense process relate, roughly speaking, to the collection of data from Portuguese citizens, within the scope of the 2021 Census activity.

47. Which, as can be seen from the nomenclature, took place during the year 2021, and was already concluded when the Draft Deliberation was notified.

48. Therefore, the Defendant's obligations have already been irremediably breached, and this breach has already materialized - and expired - until the conclusion of that activity, in the year 2021.

49. The useful effect of a prior warning is not achieved to have a treatment corrected or terminated when it is no longer in progress, as it has already been completed.

50. The ratio legis of this provision is to ensure the correction of the infringement, when there is the possibility for the controller to correct his conduct, thus reducing the risks for the legal sphere of the holder of the personal data.

51. Something that, in casu, would no longer be, nor is, possible to achieve.

52. It should also be noted that the norms must be interpreted taking into account the rules for the interpretation and application of laws, which invite one to also assess, among other aspects, the intention of the legislator (cf. articles 1,° to 13 of the Civil Code).

53. The interpretation of the law should not be limited to exploring only the literal meaning of the provisions.

54. Now, if the infringement has already been consolidated, and it is not possible to prevent its occurrence or the damage that the breach of the Defendant's obligation produced in the sphere of the holder of personal data, it makes no sense to call for the application of a prior warning.

55. Regardless, even if it were applicable, the CNPD decides not to apply the provisions of article 39(3) of Law No. 58/2019, of August 8, in the present case, by virtue of the principle of the primacy of European Union Law and with the foundations contained in Deliberation/2019/494, of September 34, since such rule, by imposing on the CNPD a previous step to the decision to open a sanctioning procedure, which is embodied in a warning for the correction of the illegality within a reasonable period, establishes

4 Accessible at https://www.cnpcl.pt/bin/decisoes/Delib/DEL 2019 494.pdf

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

í

a special regime for unlawful conduct committed with negligence that is not compatible with the regime provided for in the RGPD.

56. In reality, as is clear from the body of Article 83(2) of the GDPR, the EU legislature grants the specific decision-maker, depending on the circumstances of each case, a discretionary power to apply fines in addition to or in instead of the measures

referred to in points a) to h) and j) of Article 58(2) of the GDPR.

57. Indeed, by determining that '[depending on the circumstances of each case, the fines are imposed in addition to or instead of the measures referred to in Article 58(2)(a) to (h) and j) [.. .]', Article 83(2) of the GDPR grants national supervisory authorities the power, on a case-by-case basis, to opt for the application of a fine only, the application of a fine and corrective measure, or the isolated application of one or more measures corrective measures provided for in paragraph 2 of article 58. It is this discretionary power that is indisputably attributed to the national control authorities, which the rule contained in Article 39(3) of Law No. 58/2019 is restricting, imposing in abstract the CNPD the adoption of a specific measure, regardless of the circumstances of each case (since it only takes into account the negligent nature of the infraction) and without allowing the immediate application of a sanction to be cumulated.

58. However, such an imposition deprives the supervisory authority of the discretionary power recognized by the RGPD, removing or considerably reducing the useful effect of the rule that attributes it5.

59. In addition, the national legislator cannot impose on its supervisory authority the adoption of a corrective measure, determined in Article 58(2)(a) of the RGPD for situations in which a data processing operation is foreseen. data (therefore not yet implemented) that is likely to violate the rules of the Regulation, in situations where the assumptions of that measure are not met. In other words, if the RGPD defines, in paragraph a) of paragraph 2 of article 58, the assumptions of the warning decision, national law cannot impose the practice of this act when there is a situation that does not fall under those assumptions and fulfills another legal type for which the RGPD provides for a decision with the same designation.

5 Incidentally, the national legislature seems to intend to recover a provision foreseen in the first version of the proposal for a regulation authored by the European Commission (then Article 76, paragraph 3), which was eliminated in a later stage of the European legislative procedure, which constitutes yet another argument in favor of the interpretation that the Union legislator refused to limit or abstractly empty the powers of application of pecuniary sanctions to the infractions provided for therein, so that a national rule that provides for such a prior procedure for any and all infractions negligent with the effect of postponing or making it impossible to exercise the sanctioning power recognized by the RGPD undermines the useful effect of the Union rule that provides for such powers, putting into crisis the principle of effectiveness of Union law.

60. In the light of such arguments, the CNPD does not apply in the present case paragraph 3 of article 39 of Law no. 58/2019, of 8 August.

61. Moreover, the limited understanding of the principle of legality of administrative activity, revealed by the Defendant in point 186 of the Defense, is not followed, as it is not consistent with the current legal-constitutional framework.

62. The principle of legality, enshrined in article 266 of the CRP, is today affirmed as a principle of legality, in the sense that the Public Administration is bound by the different heterodetermined normative provisions and, therefore, determined not only by the national legislator but also by the legislator of the European Union; as, moreover, it follows from paragraph 4 of article 8 of the CRP, which integrates Union law directly into the national legal order. And, in the application of internal and Union legal norms, the principle of the primacy of Union law cannot fail to be considered, as it has been interpreted by the Court of Justice of the European Union, which obliges the non-application of internal legislative norms whenever that they contradict Union law or undermine its practical effect.

63. And the Defendant should not claim that the CNPD, as an administrative entity, does not have the competence to disregard the rule in question.

64. For it is important to recall the understanding of the Constitutional Court, expressed recently in judgment no. 268/2022, commonly known as the Metadata Judgment, which reads:

"As a result, any conflict between the norms now in crisis and the rules of law of the European Union that may be invoked internally will have the response of the national judicial system to the non-application of internal norms - without these being purged from the legal system or generating , for this purpose, its invalidity. It was precisely what the National Data Protection Commission (CNPD) decided: considering in its deliberation n.0 641/2017, of May 9, 2017. ° 32/2008 is contrary to European Union law - for disproportionate transgression of articles 7 and 8 of the CDFUE - decided to disapply Law 32/2008, based on the primacy of European Union law fDeliberation n.0 7 008/2017 , of July 18, 2017)." our underlining.

65. Subsequently, that Court renewed this understanding, in Judgment No. 382/2022, which reads:

"4. Secondly, it will always be said that the grounds invoked for the nullity of Judgment No. 268/2022 are manifestly unfounded.

On the one hand, because the rules that determine an undifferentiated obligation to conserve metadata could no longer be applied by any national authority since 2014, when it was concluded that they were incompatible with the Charter of Fundamental Rights of the European Union (Judgments of the Court of Court of the European Union of April 8, 2014, Digital Rights Ireland, case C-293/12 and C-594/12; and of December 21, 2016, Tele2 Sverige and Watson, case C-203/15 and C-698/15) and the obligation arose for all national authorities (including the judiciary) to refuse its application, pursuant to the provisions of Article 8(4) of the Constitution and as decided by the National Commission for Protection of Data in Deliberation No. 1008/2017. of July 18, 2017." - our emphasis.

66. In other words, the CNPD not only has the power to decide on the non-application of norms that are in contradiction with European Union law, but it also has the obligation to do so, so that, in these terms, there is no violation of the principle of legality.

67. The Defendant also adds, in paragraph 182 of the Defense, that "[...] the rules contained, namely, in article 83 of the RGPD, cannot be interpreted in the sense of directly targeting the competent national control authorities, inasmuch as, pursuant to the provisions of article 83, paragraph 9, sanctions provided for in the RGPD are only applicable 'when the legal system of the Member States does not provide for fines', which are 'effective, proportionate and dissuasive' ".

68. Now, the Defense reveals a wrong reading of the RGPD, and ignorance of recital 151 of the same European law. In fact, Article 83(9) of the RGPD aims to remedy the non-existence of fines "as provided for in the [RGPD]" in the legal systems of Denmark and Estonia, as explained in that recital, which only reinforces that article 83 is addressed to the actual applicators of sanctions, that is, the national supervisory authorities and the courts - as the CNPD mentions in the determination cited by the Defendant (Deliberation 2019/494).

69. Furthermore, what was stated in point 183 of the Defense does not add anything to the Defendant's arguments, corresponding to the mere finding of a norm that spells out the principle of the rule of law; on the contrary, it reveals an irremediable contradiction in the Defendant's argument, since Article 83(8) of the GDPR specifically states that this article is

addressed to the national supervisory authorities ("[the] exercise of the powers conferred upon it by this Article by the supervisory authority [...]").

AVG/2021/4017

Cif»

National Data Protection Commission

iv. Nullity of the Deliberation Project due to violation of the Defendant's technical independence

70. The Defendant claims that technical independence constitutes a basic principle of official statistical activity, which is established in national and European legislation.

71. This is why the Defendant, in the pursuit of his public interest mission, can freely define statistical processes, methods, standards and procedures, without being subject to any external interference, namely by any other administrative authorities.

72. Therefore, according to the Defendant's understanding, the definition of personal data processed within the scope of the Census 2021 census activity, as well as the respective processing of the data, is his exclusive competence, not being susceptible to being syndicated by other administrative authorities.

73. With this argument, he concluded that the CNPD does not have the competence to indicate the suitability, pertinence or need, nor the methodologies and procedures for collecting and processing data for statistical purposes.

74. In doing so, the Defendant considers that the Draft Deliberation will have to be void.

75. That argument is unfounded.

Let's see,

76. Firstly, at no time is the Draft Decision called into question - as the Defendant alleges, several times throughout the Defense -, the regulatory and institutional framework (national and European) under which the activity was carried out Census 2021.

77. Nor the technical independence of the Defendant in carrying out that census activity.

78. In fact, and as explained above, at no point in the project does the CNPD question or censor the statistical variables defined by INE, nor the option of collecting data via the Internet.

79. What the CNPD verified, and is currently analyzing, is not whether those variables are necessary for the census activity - given that the judgment of need was explicitly attributed to INE by national law -, nor the methodology and procedure of

collecting such data.

80. On these aspects of the census operation, the CNPD spoke within the CSE, either at meetings of this council or at SEAC, recognizing the legal limits to the fulfillment of its mission in this headquarters. Even so, he did not fail to affirm the intrusive nature of the collection of information relating to religion and warned of the specific risks arising from the online collection of responses to surveys.

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

81. Specifically regarding the variables that correspond to special categories of personal data, the CNPD does not question the competence and technical autonomy of INE for defining them and for their treatment, under the terms recognized by paragraph 2 of article 18. of the Law on the National Statistical System.

82. And, therefore, it is not achieved because INE was tired in a long argument in points 329 to 377 of its Defence.

83. But the fact that the law recognizes INE's technical autonomy to define the variables necessary to pursue the statistical public interest and legitimizes it to process the corresponding personal data, does not mean that INE can demand citizens to provide such data when they fall under the category of special or sensitive data (sensitive personal data not only relating to respondents but also to members of the respective household).

84. In fact, the same Law of the National Statistical System, in paragraph 3 of article 4, is clear in excluding categories of sensitive personal data from the information whose supply may be required, as mandatory, by INE.

85. It is this aspect of the processing of personal data that the CNPD analyzes and highlights for administrative purposes: the fact that sensitive personal data were presented as being mandatory for respondents, when the law imposes the optional nature of its collection and establishes a set of information obligations towards respondents (cf. paragraphs 3 and 4 of article 4

of the Law on the National Statistical System).

86. In short, with regard to the variables that correspond to special categories of data, only one aspect of the processing of personal data is at issue that is not covered by the technical autonomy of INE, but is rather legally defined - by the System Law itself National Statistician - and, therefore, the verification of respect for such a condition or legal link to the processing of personal data is, obviously, up to the CNPD.

87. At the same time, the fact that the respondents and the members of the respective household have to be identified by their full name goes beyond the technical autonomy that the law recognizes to INE, contrary to what the Defendant states in point 326 of the Defence.

88. This is an aspect of the processing of personal data that national and European legislation does not specifically assign to INE, nor does it qualify as part of its technical autonomy. And it does not, because, in reality, it is the personal data protection regime that imposes the minimization of personal data and the mitigation of risks to the rights of holders here.

89. In fact, the respondents' identification data are not part of the concept of a statistical variable (cf. Annex to Regulation (EC) 1201/2009, of November 30, 2009), and are therefore not subject to technical autonomy of INE, being, therefore, an aspect of data processing, in the context of the census operation, which the CNPD can supervise and assess from the perspective of its compliance with the principles of data protection.

90. Just consider the provisions of Article 18(5) of Decree-Law No. 54/2019, where, although INE is recognized as competent to assess the need for personal data in the information collected from databases administrative, except for the powers legally attributed to the CNPD in this context.

91. Furthermore, the fact that INE enjoys autonomy and technical independence for the definition of technical solutions, within the regulatory and institutional framework - national and European - does not imply that the Defendant's behavior is no longer subject to respect by others diplomas of the Portuguese legal system.

92. Autonomy and technical independence are not synonymous with legality or activity exempt from regulation, and therefore

have to be framed by the legal regimes applicable to census activity, as is the case with the legal regime for the protection of personal data.

93. In other words, it is not because the Defendant's technical autonomy is recognized, in statistical matters, that he is no longer subject to respect and fulfillment of legal obligations resulting from numerous legal diplomas and, therefore, from the Constitution of the Portuguese Republic , the European Charter of Fundamental Rights of the European Union and, of course, the GDPR.

94. Admitting that, as technical autonomy was recognized, the Defendant's conduct could not be subject to any external control - as seems to be the understanding postulated in the Defense - would be to admit that statistical activity would be removed from the bonds of the rule of law.

95. Namely, and within the scope of his technical autonomy, the Defendant could disrespect the rights of Portuguese citizens enshrined in the CRP, provided that his action was aimed at carrying out a census operation - which cannot be conceived.

96. Therefore, it is concluded that, notwithstanding technical autonomy, when carrying out statistical activities, the Defendant is still subject to respect for the applicable legal norms and their inspection by the competent authorities.

97. As we have already seen, in this case, the CNPD is competent to ensure compliance and monitor compliance with the rules contained in the RGPD.

98. For this reason, the Defendant cannot, due to its technical autonomy, frustrate its decisions and actions regarding the processing of personal data to the investigation by the CNPD.

99. Also because, if that were possible, the CNPD would no longer have powers and competences vis-à-vis any public entity endowed with autonomy or technical independence.

100. In this matter, attention should be drawn to the provisions of Regulation (EC) 763/2008, of July 9, 2008, on population and housing censuses, which exhaustively establishes in article 4, on the heading "Data Sources", the following:

"7- Member States may compile their statistics from different data sources, in particular:[...]

2- Member States shall take all necessary measures to comply with data protection requirements. This Regulation does not affect Member States' legislation on data protection." - emphasis added.

101. In addition, the same obligation to respect the RGPD, in the execution of the 2021 Census operation, is expressly enshrined in Decree-Law no. 54/2019, of April 18, which reads, in paragraph 4 of article 4th, the following:

"4- The answers to the 2021 Census questionnaires are kept by INE, I.P., under conditions of absolute security, and can only be used for exclusively statistical purposes, in compliance with the provisions of Law n.0 22/2008, of May 13, and in Regulation (EU) n.0 2016/679, of the European Parliament and of the Council, of April 21, 2016."

102. As it is known that national legislation (Decree-Law No. 54/2019, of April 18) cannot contradict the provisions of Regulation 763/2008, the combination of the two aforementioned rules, it is clear that the Defendant must comply the principles and rules relating to the protection of personal data.

103. For this reason, the Defendant's activity could never be frustrated by the CNPD's inspection, with regard to respect for the GDPR rules.

104. Although the Defendant intends to hyperbolize his concept of technical independence, to the point of acting without any need to respect legal norms - which, of course, he cannot do - legislation, national and European, subject the Defendant's performance to control and inspection by the national supervisory authority (cf. article 55 of the RGPD), which, in Portugal, is the CNPD (cf. article 3 of Law no. 58/2019, of 8 August).

105. On the other hand, the CNPD has always considered and defended that data should be collected in a format that is not based on identifying the respective holders by full name, in order to minimize the risk to the rights of citizens.

106. This was expressly assumed by the CNPD regarding the data collection model from the administrative bases, in Deliberation no. 929/2014, which the Defendant cites in his Defence, the CNPD having determined that the personal data were encoded or pseudonymized - so what is stated in point 304 of the Defense is not accurate. In that Deliberation, as well portrayed by the Defendant in points 314 to 317, it was determined that the data were collected and integrated based on

numerical identifiers, admitting, at the limit, the use of letters of the first and last name (the first three letters) - which is quite different from requiring and treating the full name of respondents or members of the respective household.

107. In the same sense, the CNPD expressed itself in Opinion No. 28/2018, of June 11, p. 4, a document that the Defendant does not ignore, and which, moreover, he cites in his Defense, where it is stated:

“It should be noted, however, that as a result of painstaking and successive work, over several years, the CNPD and INE have reached fruitful understandings for this purpose. A good example of this is narrated in deliberation n.0 129/2018, of January 30, where the CNPD addressed a data exchange protocol between the Tax Administration and INE. There, the procedures already introduced in the processing of information prior to its submission to INE were listed. Of these, the pseudonymization procedure stands out, better detailed in deliberation n.0 929/2014, which guarantees that INE, being able to relate the information received, does not, even so, have access to the identification of the data subjects.

It is precisely in this sense that we believe that the future path of making use of this administrative information must be followed, combining, in the most harmonious way possible, statistical purposes and respect for the protection of personal data".

108. In reality, the Defendant persists in trying to confuse two different concepts, equating individual data with data identified by full name, when it is certain that there are other data (numerical first) that allow the association of information to a particular citizen and that , by the way, ensure greater rigor in the relationship of personal data (since it is known that the use of the name as a connection key between the data generates errors, because of the spelling - in particular, with respect to the existing connection particles in the names) , therefore, ensuring respect for the principle of accuracy of personal data (principle enshrined in Article 5(1)(d) of the RGPD). In other words, it's

possible to individualize the information in terms that allow the relationship with other information relating to the same subject, without resorting to data directly identifying the data subject.

109. As, incidentally, it confuses or intends to confuse the identifiability of respondents (and household members), through

certain identification data, with their identification by full name (as happens, again, in point 889 of the Defence).

110. The argument of the absence of a unique citizen number - invoked in point 309 of the Defense - does not determine that citizens have to identify themselves by name, in order to be able to aggregate the information existing in the Public Administration databases. The constitution of an individualized database referred to in paragraph c) of article 3 of Law no. 54/2019 does not require, contrary to what the Defendant states, the collection of the full names of citizens - being this is inaccurate what was stated in point 312 of the Defense.

111. Incidentally, the work carried out by the CNPD and the INE, in the context of the procedure that gave rise to the aforementioned Deliberation 929/2014, aimed to ensure that the census operation did not depend on the collection of the full name, so that the Defendant cannot ignore the pseudonymization technique, nor the various paths that the CNPD has pointed out to it towards this pseudonymization.

112. In short, the arguments of the Defendant, in this matter, cannot, of course, be accepted.

v. Violation of the principle of ne bis in idem

113. The Defendant alleges that the imputation of four of the administrative offenses contained in the Project - and identified by the Defendant in point 211 of the Defense - violate the legal-constitutional principle established in paragraph 5 of article 29 of the CRP and in article 4. ° of Protocol No. 7 to the European Convention on Human Rights, which prohibits double punishment for the same offense.

114. In order to try to demonstrate such double punishment, the Defendant alleges that he is charged with committing an administrative offense for violating the provisions of Article 5(1)(a) of the RGPD and is likewise charged with an administrative offense for violating the provisions of Articles 12 and 13 of the GDPR.

115. The Defendant considers that Articles 12 and 13 of the RGPD are a mere specification of the principle contained in Article 5(1)(a) of the RGPD, and therefore cannot be punished twice.

116. According to the Defendant, so much so that the Draft Deliberation describes the same factuality that is relevant to consider the objective type of offense verified, that is, the failure to provide information to holders in a concise, transparent, intelligible and easily accessible manner.

.... D

National Data Protection Commission

117. It also adds that it must be concluded that the conviction for any of the alleged offenses already expresses the legal worthlessness of the behavior.

Let's see,

118. We agree with the Defendant when he alleges that sanctioning the violation of obligations set out in the RGPD and which correspond to the intensification of some of the principles enshrined in Article 5(1) of the RGPD should rule out sanctioning the violation of the RGPD itself principle.

119. This is the case with regard to the relationship between paragraphs a) and c) of paragraph 1 of article 5 of the RGPD and article 9 of the RGPD, which appeared in the indictment as separate offences, which is now reviewed.

120. Thus, the CNPD does not sanction, after all, the violation of the principle of loyalty, nor the principle of minimization of personal data, focusing on the violation of paragraph 1 of article 9 of the RGPD, due to lack of grounds for lawfulness for the processing of special data of optional collection.

121. But it maintains, as it is autonomously cut by the Union legislator, in articles 12 and 13 and in subparagraph b) of paragraph 5 of article 83 of the RGPD, the violation of the right to information regarding the set of the processing of personal data carried out in the context of the census operation.

122. Reason why the alleged by the Defendant only partially succeeds.

saw. On the existence of legal basis for the treatment of special categories of data

123. The Defendant understands that the imputation directed at him, arising from the illicit processing of data of special categories, is based on an inadequate understanding of the nature of the data to which questions 29.3 to 29.6 and 30 relate.

124. The Defendant also alleges that he exercises public interest functions in the field of official statistical activity, so that there is a legal basis for the processing of those data.

125. Regarding the question regarding the degree of difficulty felt in carrying out activities by the respondents, in the Defendant's understanding, this does not constitute a special health data, as it is not questioning what type of problems or illnesses the data subject has or from which he suffers.

126. It also invokes Authorization No. 2600/11, of March 24, 2011, to claim that items 29.3 to 29.6 do not constitute data

relating to health.

Av. D. Carlos 1,134,1o 1200-651 Lisbon

T(+351) 213 928400 F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

v.

r

127. Subsequently, the Defendant alleges that, as a national statistical authority, its activity falls within the scope of paragraph j) of paragraph 2 of article 9 of the RGPD, so that, as it pursues statistical purposes of public interest, it does not requires the consent of the data subject for that treatment.

128. Invoking, to support its position, CNPD Opinion No. 28/2018.

129. The Defendant considers that this conclusion also leads to the provisions of paragraph 2 of article 18 of the National Statistical System Law (Law No. 22/2008, of May 13), although with the caveat that within the scope of that Law, data referring to philosophical or political convictions, party or union affiliation, religious faith, private life and ethnic origin and personal data relating to health and sexual life, cannot be mandatory.

130. However, it states that the personal data contained in questions 29.3 to 29.6 and 30. were treated as an optional answer.

131. The Defendant also argues, further on in his Defence, that in the statistical variables included in questions 29 and 30, there was a notice in the header, in the form of a banner informing the optional nature of all subsequent questions.

132. This information being provided to the data subject, either in the printed form or in the online form.

Let's see,

133. In light of the RGPD, it is not understood how the Defendant can currently consider that the collection of personal data that allows identifying whether someone has difficulties in locomotion, concentration, dressing or bathing, or that expressly indicate a given religion , do not constitute special categories of data, as specified in Article 9(1) of the RGPD (cf. point 244 of Defense).

134. Indeed, under the terms of the RGPD, personal data are special categories, and it is quoted, “that reveal racial or ethnic origin, political opinions, religious or philosophical convictions, or trade union affiliation, as well as the treatment genetic data, biometric data to uniquely identify a person, data relating to health or data relating to a person's sex life or sexual orientation" (cf. Article 9(1) GDPR).

135. It is important to emphasize that the Defendant, also in what he considers to be valid arguments for his defense, shows the weaknesses in monitoring the regulatory changes operated with the entry into force of the RGPD, considering that the individual form of the 2021 Censuses should be had

as valid because it was written in terms entirely congruent with the 2011 Census form (cf. points 240 and 241 of the Defense).

136. In fact, article 7 of the Personal Data Protection Law (Law No. 67/98, of October 26) provided for a regime for the processing of sensitive data which, despite some similarities, is not identical to the enshrined in article 9 of the RGPD, given that the fact that the Defendant considers the existing congruence between the 2011 and 2021 Census forms to be an argument in favor of his defense demonstrates a total lack of knowledge and high disregard for the legal data protection regime current.

137. If it is true that the CNPD, in Authorization No. 2600/11, of March 24, 2011, did not consider that that information to be subsumed under the concept of health data, it is no less true that the RGPD came to explicitly define the concept of "health data" in Article 4(15) of the GDPR.

138. In view of such a legal definition, it cannot but be considered that personal data relating to difficulties in locomotion, concentration, dressing or bathing correspond to "personal data related to the physical or mental health of a natural person" (Article 4(15) of the GDPR) or "[...] data relating to the state of health that reveal information about your physical or mental health in the past, present or future. The foregoing includes information about a natural person [...], for example, an illness, disability, a risk of illness [...Jou physiological or biometric state of the data subject, regardless of its source [...] " (cf. recital 35 of the RGPD) and therefore are personal data relating to health.

139. Therefore, the argument presented by the Defendant, which is based on an understanding of the CNPD expressed in

2011, does not apply, when, however, a profound reform of the legal regime for the protection of personal data took place, a reform that the Defendant cannot ignore - in particular , after the European Data Protection Board clarified this concept (cf. point 3.1 "Data concerning health" of "Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak"6).

140. All the more so as it is the Defendant himself who, in the survey made available to citizens in the 2021 Census operation, refers to such data as variables related to "health problems" (cf. image Q3.29.1. of the annex "Captures of screens from the 2021 Census form, available at https://censos2021 .ine.pt" to the report "Info UI AVG 2021 401 II vl.O.docx").

141. Thus, it is now indisputable that the data provided for in questions 29.3 to 29.6 and 30 of the survey are special personal data, under the terms of paragraph 1 of article 9 of the RGPD, so that their collection is not sufficient with the

6 See https://edpb.europa.eu/sites/default/files/files/fiie1/edpb_guidelines_202003_heaithdatascientificresearchcovid19_en.pdf

the need for these personal data for the pursuit of the public interest by INE (i.e., not being sufficient to fulfill the condition provided for in subparagraph e) of paragraph 1 of article 6 of the RGPD), still depending on the verification of one of the conditions provided for in Article 9(2) GDPR.

142. It is agreed with what is alleged in the Defense that the processing operations in question are supported, for legal purposes, in the public interest. However, as the CNPD warned in a timely manner in its Opinion No. 28/2018, of June 11 (p. 1 v), not unrestrictedly. It is true that the pursuit of a public interest legitimizes the processing of special categories of data for statistical purposes "[albeit not unrestrictedly, since such processing "must be proportionate to the aim pursued, respect the essence of the right to protection of personal data and provide for adequate and specific measures for the defense of the fundamental rights and interests of the data subject.»" - opinion, moreover, quoted by the Defendant in her Defense.

143. Therefore, the legal classification of the facts committed by the Defendant is changed, accepting that the lawful basis for

the processing of personal data is not consent under the terms of Article 9(2)(a) .° of the GDPR.

144. However, it is not ignored that the Law on the National Statistical System (Law No. 22/2008, of May 13), in Article 4(1), recognizes the power of INE to demand the provision, with mandatory nature of personal data, unless these are part of the special categories of data (cf. paragraph 3 of the same article), in which case such provision depends on the will of the data subjects.

145. Furthermore, the INE has the obligation to inform respondents of the mandatory or optional nature of the response to questions relating to sensitive data (cf. no. 4 of article 4 of the Law on the National Statistical System).

146. It follows, therefore, that the national legislature, in balancing the public interest associated with statistical activity, on the one hand, and the fundamental rights to informational self-determination and privacy, on the other hand, considered it excessive to impose the provision of sensitive personal data, thus making its collection dependent on the will of the respective holders.

147. Thus, even if it is claimed to be point j) of paragraph 2 of article 9 of the RGPD or, perhaps, point g) of the same number, the basis for the lawfulness of the collection of personal data in this statistical operation , the truth is that, given the requirement - today reflected in those paragraphs as well as in article 89 of the RGPD - that the forecast of the treatment be accompanied by adequate measures to guarantee the proportionality of the treatment in relation to the intended objective, the minimization of data personal data and respect for the rights of data subjects, the national legislator has explicitly established, as an appropriate measure, the dependence on a manifestation of will by the subject regarding the collection of sensitive data.

148. Thus, the realization of the public interest is conditioned to the will of the data subject. And therefore, the public interest is clearly not sufficient to legitimize the collection of data provided for in paragraph 1 of article 9 of the RGPD, which is why it is not lawful to collect such data that, due to lack of information, does not allow the free formation of the will of the respective holder.

149. And the point is that, even though INE was aware that special data relating to health and religion could only be collected

on an optional basis, the fact that it did not provide clear and complete information about the optional nature of its provision by citizens, in disrespect for the legal obligation provided for in paragraph 4 of article 4 of the Law on the National Statistical System, impaired the understanding by respondents that questions 29.3. to 29.6. and 30. of the 2021 Census questionnaire were optional.

150. It should be noted that, for the purpose of verifying the legal assumption that the collection of this special or sensitive personal data is optional, it is not the conviction of INE (contrary to what the Defendant intends in point 259 of the Defense), but rather, the conviction of the respondents: the legal assumption, defined in paragraph 3 of article 4 of the Law on the National Statistical System, is that respondents want to provide such data to INE. And wanting depends on a free formation of that will, not conditioned by omission of information or provision of incomplete or erroneous information.

151. To that extent, the mere de facto possibility of navigating the online form continuing in the absence of a response to such questions - which was not allowed by the system in the mandatory questions - and even of proceeding to hand in the questionnaire without filling in the answers to the questions 29.3. to 29.6. and 30. of the 2021 Census questionnaire (cf. as invoked in points 266 and 267 of the Defense) is irrelevant for the purpose of forming the will of the respondents, since, in the absence of information about the optional character of the answer to those questions, it is not even expected, let alone required, that they would try to continue navigating the form or submitting it without filling out those answers.

152. In fact, as mentioned in the Draft Deliberation and not contested by the Defense, in the online questionnaire:

"Question 30 was optional. However, it did not provide any information about the non-mandatory nature of the answer."

"Point 29 of the questionnaire consisted of six questions framed in three pages, with two questions on each of them. Only on the first of these pages was information given about the optional nature of the answers. ". [...]". (cf. images Q3.29.1 to Q3.30, in the annex "Captures of the screens of the

2021 Census form, available at https://censos2021 .ine.pt" to the report "Info UIAVG 2021 401 II v1.0.docx").

153. It must be concluded that the fact that the system allows navigating to the next page without selecting an answer does not guarantee the data subject information regarding the optional nature of the question presented.

154. Also because, remember, the data subject is answering the questionnaire to avoid being sanctioned, which at the outset leads him to consider all the questions presented in the form as imperative.

155. That is, the data subject hardly tests the possibility of moving on to the next question without previously responding to the previous one.

156. Being logical the difficulty of apprehending the optional nature, if this information was not included on the screen of questions 29.3. to 29.6. and 30.

157. The truth is that the lack of information about the optional character of the 29.3. to 29.6. and 30. of the 2021 Census questionnaire generated or, at least, is likely to have generated the conviction that answering them was mandatory, with which the effective response to those questions by respondents cannot correspond to a manifestation of free will, since it was, or may have been, based on an error regarding the mandatory nature of the provision of such data.

158. It follows from the general rules of law that the expressed will is only legally relevant and valid if freely formed and manifested, and that the error harms this freedom, especially when it affects an essential element of the will: the mandatory nature of the conduct dependent on the manifestation of will.

159. Now, in this case, the error in forming the will of the respondents is caused by the INE, by not having fulfilled the requirement of no. 3 of article 4 of the Law on the National Statistical System.

160. Therefore, the Defendant is in error when, in points 261 and 262 of the Defense, he considers that these two issues are distinct, that is, the lack of information about the optional nature of the questions and their optional nature; on the contrary, in this context, they cannot be separated, because that is what the national legislator wanted, in the Law on the National Statistical System (cf. paragraphs 3 and 4 of article 4), when he made the lawfulness of data collection dependent on sensitive personal data of its optional nature and the provision of information about this optional nature.

161. In these terms, the collection by INE of special personal data through the response to questions 29.3. at 29.6. and 30. of the 2021 Census questionnaire was illegal, because, under the terms of paragraph j) (or even g))

of paragraph 2 of article 9 of the RGPD, the national legislator, in article 4, paragraphs 3 and 4, of the Law on the National Statistical System, when it provided for the collection of special data for the purpose of interest statistical public established, as an adequate and specific measure for the defense of the fundamental rights and interests of the data subject, the optional character of the same, thus requiring the manifestation of an informed and free consenting will, which, in the case, was not verified by lack of provision of clear and complete information on all questions that were optional.

162. In view of the above, the Defendant's understanding cannot be accepted, maintaining that the collection of such personal data violated the prohibition contained in Article 9(1) of the RGPD, as none of the conditions of legality provided for in paragraph 2 of the same article.

vii. Violation of the principle of minimization of personal data

163. The Defendant alleges that he does not infer from the Draft Decision whether the imputation formulated concerns the delimitation of the information to be obligatorily provided to the data subject - a matter that, according to him, would fit, only, in the legal framework related to the principle of transparency and the fulfillment of the information duties - or if an infraction resulting from the processing of data of special categories is also imputed to him.

164. Even so, it argues that a possible failure to provide information about the optional nature of the answers to questions 29.3 to 29.6 and 30. would constitute an offense only likely to be framed within the framework of the respective duty to inform, as the questions were treated as being optional .

165. That is, the Defendant seeks to justify that the data collected in response to questions 29.3 to 29.6 and 30. did not involve a violation of the principle of data minimization, under the terms and for the purposes of the provisions of subparagraph c) of paragraph no. 1 of article 5 of the RGPD, as they are essential and justifiable in the light of statistical needs and numerous international recommendations produced by reference entities, in census matters (cf. points 329 to 377 of the Defense).

166. Regarding this point, the CNPD concedes that this fact does not correspond to a violation of that principle. This does not exclude its relevance for the purpose of verifying the non-fulfillment of the legality condition under the terms of paragraph 2 of article 9 of the RGPD, in the terms set out above.

viii. The Defendant complied with the information duties towards the holders of personal data

167. The Defendant claims to have provided the data subjects with all the necessary and required information, under the terms and for the purposes of Article 5(1)(a), in conjunction with the provisions of Articles 12 and 13 of all GDPR.

168. Even so, the Defendant understands that he fulfilled all the information duties, both in the printed version and in the digital version.

169. It alleges that, for this purpose, it made its Privacy and Personal Data Protection Policy available on its website, under the terms of which are the contacts of INE and EPD, from which the holder could obtain further clarification.

170. The Defendant also argues that in the statistical variables included in questions 29 and 30, there was a notice in the header, in the form of a banner informing the optional character and all subsequent questions.

171. This information being provided to the data subject, either in the printed form or in the online form.

172. Furthermore, the Defendant considers that the online system itself led to the conclusion that the questions were optional, since it allowed navigating to the next page without selecting any answer, which was not allowed by the system in the mandatory questions.

Let's see,

173.As for the duty to provide information on the optional character of special data, the arguments presented above have already been refuted, granting now, only, that its non-compliance is consumed by the lack of grounds for the lawfulness of the collection of such data, since that it is a specific requirement of the GDPR rule that INE invokes to legitimize your treatment.

174. However, the question of whether the duty to provide information under Article 13 of the GDPR has been fulfilled is different.

175. It is important to clarify that the duty to provide information provided for in Articles 13 and 14 of the RGPD aims to implement the principles of transparency and loyalty, enshrined in Article 5(1)(a) of the RGPD.

176. Articles 12 and 13 of the RGPD are clear in requiring the controller to provide the data subject with information in a

"concise, transparent, intelligible and easily accessible manner, using clear and simple languagej.. .]".

AVG/2021/401 14

í

D

National Data Protection Commission

177. Contrary to these legal commands, the Defendant chose to inform data subjects through a document available on its website.

178. However, this document refers to all processing of personal data under the responsibility of INE and not specifically to the processing resulting from the census operation, being silent about this - in fact, it is enough to see that the so-called Privacy and Data Protection Policy Personal is dated 2019, more than two years before the said operation was carried out.

179. In addition, the location on Statistics Portugal's institutional website of the aforementioned privacy policy makes it, in practice, inaccessible.

180. Otherwise, let's see: to find it, it is necessary to go to the bottom of the page, and select "About INE" - knowing that, for the common citizen, it is not expected that the privacy policy is stored there; even after accessing the "About INE" link, the "Ethics and Policies" tab must be opened, so that, after selecting the seventh of eleven options, one can navigate to another page where a small text appears, which, by in turn, it refers to a PDF document which contains, finally, the so-called Privacy and Personal Data Protection Policy.

181. There is a clear lack of transparency in the processing of personal data carried out by INE and, specifically, regarding the processing of data from the 2021 Census, in view of the complex and labyrinthine path that citizens have to take, almost requiring them to have divinatory qualities, to find the information required by law.

182. Especially because, in the case of the census operation Census 2021, what the data subject wanted was to access a form, in order to respond and avoid being sanctioned for the lack of response, insufficiency or inaccuracy of the same.

183. And it is the Defendant himself who mentions that that same form did not contain the information to which he was legally obliged, pursuant to the provisions of Articles 12 and 13 of the RGPD.

184. Now, as the direct collection of personal data is at stake, paragraph 1 of article 13 of the RGPD requires that the controller at the time of collection provide the information listed there, which manifestly did not occur.

185. Nor was the requirement to provide information in a concise, transparent, intelligible and easily accessible manner, pursuant to paragraph 1 of article 12 of the RGPD, not been complied with.

186. From all of the above, it must be concluded that the Defendant did not comply with the information obligations to which he was bound, thus violating the obligation arising from Articles 12 and 13 of the RGPD.

Av. 0. Carlos 1,134,1o

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

ix. Breach of due diligence in choosing subcontractor

187. The Defendant considers, in his Defence, that the services subcontracted to Cloudflare, Inc, respect all information security and personal data protection requirements, as provided for in the RGPD and other legislation on data protection.

188. And, therefore, they constituted the best option for the success of the Census 2021 census operation in good time and with greater security and better performance of technological services and infrastructure, in the face of expected global threats.

189. The contractual relationship established between the Defendant and the subcontractor was governed by a contract between the parties, which includes clauses containing all the information and obligations legally required pursuant to Article 28(3) of the RGPD.

190. Furthermore, the Defendant alleges that there are not numerous alternative solutions available on the market that provide performance and security services with the level of excellence, rigor and concern for the security and privacy of personal data, such as the subcontractor.

191. And the Defendant concludes that the solution contracted between him and the subcontractor not only allowed for increased security of the information collected and a better performance of the Censos 2021 website, through the use of services of excellence recognized as such in the market, but also it appears the existence, and consequent need, of any other solutions available on the market that could have been contracted.

Let's see,

192. In his Defence, the Defendant was unable to add anything to what was found during the inspection process, which led, in fact, to the order to suspend the sending of personal data from the 2021 Census operation to the United States of America (hereinafter USA) and to other Third States without an adequate level of protection, either through Cloudflare, Inc., or through any other company, within a maximum period of 12 hours (cf. point 42 of Deliberation 2021/533, of April 27, of CNPD, issued under the powers conferred on it by Article 58(2)(j) of the RGPD).

193. As the CNPD has already clarified, in point 76 of Directive no. 2022/1, if it is true that the relationship between controller and processor and between this and other processors must be regulated in writing (cf. no. s 3 and 4 of article 28 of the RGPD), the verification of the requirements contained in article 28 of the RGPD must be substantive and not just formal, not being limited to the choice of any standard clause.

194. For this reason, when selecting the subcontractor and the means it makes available for data processing (for example, services, products, tools, technologies), the controller

c_®

National Data Protection Commission

processing had to apply or require the contracting party to adopt appropriate measures to protect personal data and to mitigate the risks arising therefrom.

195. And the Defendant's defense proves that he did not carry out the necessary due diligence to ensure the adoption of measures capable of guaranteeing respect for the principles and rules of the RGPD.

196. It will suffice to check paragraphs 457 et seq. of the Defense to conclude it. On these points, the Defendant justifies the choice of solutions from Cloudflare, lnc.; because this company is almost the only reference in the market.

197. However, this is not true, as there are several European companies that provide Content Delivery Network (CDN) services that meet the requirements of the RGPD.

198. Nor can the Defendant base his choice on the Cloudflare service,

Inc., in the fact that it has an office in Lisbon (cf. points 642 et seq. of Defense), when the contract was signed with the

company based in the USA and, under the contractual terms, the forum for settling disputes between INE and Cloudflare, Inc. is the California Court.

199. Furthermore, the latency service subscribed to by INE, in the contract, makes it clear that, as demonstrated in the Draft Deliberation, it will be supported on numerous servers located in various geographies, most of them located outside the European Union and in jurisdictions that are not compatible with European law.

200. For greater clarity of the reasons for this determination, the CNPD recalls here that in the contract entered into, in the form of a "Business" package, governed by the "Self-Serve Subscription Agreement" and by the addendum relating to data processing (Data Processing Addendum version 3.0, dated October 1, 2020), which is part of the contract (which was available on the Cloudflare, Inc. website, in April 2021, and which corresponds to evidence No. 66 filed in the Defense), it is stated "(...) [in connection with the Service, the parties anticipate that Cloudflare, Inc., (and its subcontractors) may handle, outside the European Economic Area (EEA) (...) certain personal data protected by European data protection legislation for which the customer or member of the Customer Group is considered responsible for the treatment (...)" - cf. point 6.1 of the Data Processing Addendum version 3.0 (in a free translation from the original, written in English).

201. That is, the contract concluded by INE and Cloudflare, Inc., allows the transit of personal data to any of the 200 servers used by it, as well as the transfer of personal data to the USA, and INE, when concluding such contract, accepted such processing of personal data.

V' f

202. In fact, under the terms of the Data Processing Addendum version 3.0, which, remember, is part of the contract, personal data of the customer (data exporter) is transferred to Cloudflare, Inc., (data importer), in the USA , using as an international transfer mechanism the standard contractual clauses based on Commission Decision 2010/87/EU, of February 5, 2010, applicable to transfers of personal data to subcontractors established in third countries7, which form an integral part of the

addendum and are, to that extent, subscribed by the customer (cf. paragraph m) of clause 1.1 of the Data Processing Addendum version 3.0)8.

203. Thus, by (sub)contracting the services of Cloudflare, Inc., INE, in its capacity as data controller and simultaneously a customer of Cloudflare, Inc. accepted the conditions of use of the service, including the addendum to the terms of processing of personal data, which also regulates the transfer of personal data to the USA.

204. Still in accordance with the terms of the Data Processing Addendum version 3.0, INE granted a general authorization to Cloudflare, Inc., so that it can resort to other (sub-)subcontractors, whether companies inside or outside the Group (clause 4.2)9, recognizing and accepting that it might be necessary for the provision of the service to use (sub) subcontractors established in third countries (clause 6.4)10.

205. Whether standard contractual clauses are, in general, a legal instrument for the transfer of personal data to third countries, under the combined provisions of Article 46(2)(c) and Article 46(2)(c) and Article 46(2)(c). 5 of the RGPD, it is necessary to verify, however, whether the legislation of the third State, which obviously overlaps with an instrument of a contractual nature, does not reduce or empty the guarantees offered by these clauses,

7 As stated on the Cloudflare, Inc. website, the privacy policy was revised on October 27, 2020, to "reflect" a change in the legal instrument on which the transfer of personal data from the European Union (EU) to the United States is based United States of America (USA), which ceased to be the adequacy decision of the Privacy Shield (Privacy Shield), invalidated by the Court of Justice of the European Union (CJEU), in July 2020, in the Schrems II case, to pass to be the standard contractual clauses.

8 "SCCs" mean the Standard Contractual Clauses, available here, which are the Standard data protection clauses for the transfer of personal data to processors established in third countries as described in Art. 46 of the GDPR as from time to time varied, amended or substituted by the European Commission."

9 "The Customer grants a general authorization: (a) to Cloudflare to appoint other members of the Cloudflare Group as sub-processors, and (b) to Cloudflare and other members of the Cloudflare Group to appoint third party data center operators, and outsourced marketing, business, engineering and customer support providers as sub-processors to support the performance of the Service."

9 "The Customer acknowledges and accepts that the provision of the Service under the Main Agreement may require the

Processing of Personal Data by sub-processors in countries outside the EEA, Switzerland, or UK."

10 "The Customer acknowledges and accepts that the provision of the Service under the Main Agreement may require the Processing of Personal Data by sub-processors in countries outside the EEA, Switzerland, or UK,"

National Data Protection Commission

which are precisely intended to compensate for the lack of an adequate level of protection in the country of destination of the data (cf. Articles 44 and 46 of the RGPD)11.

206. According to the Court of Justice of the European Union (ECJ), it is up to the data exporter (INE) to verify, on a case-by-case basis, with the collaboration of the data importer (Cloudflare, Inc.), whether the specific country of destination ensures a level of data protection essentially equivalent to that guaranteed by the EU, and should, if possible, adopt additional safeguards to overcome obstacles and ensure that data protection is maintained12. This obligation also stems from compliance with the principle of responsibility, enshrined in Article 5(2) of the RGPD.

207. According to the analysis of the CJEU in the Schrems II case, the legislation of the USA - which is the destination country for international transfers from Cloudflare, Inc., under the standard contractual clauses - allows interference in the fundamental rights of individuals, based on national security and public interest requirements, which may result in access to personal data transferred from the EU to the US and the use of such data in connection with surveillance programs, based on Section 702 of the FISA (Foreign Intelligence Surveillance Act) and Executive Decree 1233313.

208. The CJEU concluded that such interference is not proportionate, in the light of Union law, insofar as the scope of the limitations on the rights of individuals is not defined, there are no clear and precise rules regarding the application of these measures nor minimum requirements for protection against risks of abuse, there is no judgment of necessity, and no enforceable rights are conferred on data subjects or legal remedies, so that the limitations on data protection arising from US law do not satisfy the requirements demanded by the Charter of Fundamental Rights of the EU14 (cf. Articles 7, 8, 47 and 52, paragraph 1).

209. Therefore, it would only be possible to carry out a transfer of personal data to the US if the legislation at issue here, and

expressly referred to by the CJEU, is not directly or indirectly applicable to Cloudflare, Inc., or its (sub-)subcontractors , and even then only through the adoption of additional measures that could demonstrably prove that this legislation would not be applicable or would have no practical effect on the transfer of personal data.

11 See paragraphs 92 and 93 of the Schrems II judgment, in which the Court noted that the assessment of the existence of a level of protection essentially equivalent to that guaranteed in the EU in the country of destination of the data must be made regardless of whether a mechanism is used transfer provided for in Chapter V of the GDPR.

12 See paragraph 134 of the Schrems II judgment.

13 See paragraph 165 of the judgment cited, where the PRISM and UPSTREAM programs are cited.

14 See paragraphs 175-176, 180-185, 191 and 194 of the cited judgment.

Av. D. Carlos 1,134,1o

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

210. However, the services provided by Cloudflare, Inc., namely those contracted by INE when you subscribed to the Business Plan, place the company directly under the purview of US legislation that imposes on it the obligation to grant mass access to personal data by you treated, from the outset as a provider of electronic communications services15, without prejudice to other types of services also being covered by other provisions of the US surveillance legislation.

211. Cloudflare, Inc., recognizes in point 7 of the Data Processing Addendum version 3.0 that, in its role as a data processor, it may be subject to requests for access to personal data by third parties within the scope of legal procedures, which may be "inconsistent" with the law applicable to your customer, i.e. the GDPR. In this case, where there is a conflict of laws, Cloudflare, Inc. declares that it will immediately inform the customer, «unless such notification is legally prohibited» (cf.

paragraph a) clause 7.1)16.

212. This is precisely the case with this US legislation which prevents US companies from informing their customers of access carried out by US authorities for the purpose of gathering information on foreigners, in the context of national security activity.

213. It appears, therefore, that there is no guarantee in the contract that the personal data of citizens residing in Portugal, collected by INE through its website, within the scope of the 2021 Census, will not be accessed by the US authorities, through from Cloudflare, Inc., due to the services provided by it to INE and which imply, according to the signed contract, the transfer of this personal data to the USA.

214. Thus, what is stated in points 668 et seq. of the Defense is irrelevant, since what is at issue here is the fact that Cloudflare, Inc., is bound to comply with US legislation, which even prevents it to inform the data controller about requests for access by certain US authorities.

215. Furthermore, the explanations presented by Cloudflare, Inc., and by the Defendant, which give the "Business" service an expression that is not accepted in the subscription contract that supports it, will not be considered.

15 Cf. FISA Section 702 Amended by 50 USC § 1881a.

16 '[■■■] If Cloudflare becomes aware of any third party legal process requesting Personal Data that Cloudflare processes on behalf of Customer ir its role as data processor or sub-processor (as applicable) then, to the extent that Cloudflare Is able to identify that such third party legal process requesting Personal Data raises a conflict of law, Cloudflare will: (a) immediately notify Customer of the request unless such notification is legally prohibited; [...]"

216. When it is stated (cf. point 475 of the Defense) that each user is forwarded to the server closest to their location, in order to justify that "Portuguese" users will be forwarded, with high probability (in the expression presented, "would likely to be directed"), for servers in Lisbon, it seems to want to ignore that this will never happen if there is a saturation of the server, at a given moment, in Lisbon.

217. Something that, in massive treatment operations, such as a census operation, occurs in countless situations.

218. But neither is it correct to state that all traffic generated when accessing the "censos2021.ine.pt" website, using the Cloudflare, Inc. CDN service, would always be connected to the closest server: the one in Lisbon (cf. point 476 of the Defense).

219. The statement that the "Business" plan does not allow routing to other servers with less "load" than the one in Lisbon (cf. point 477 of the Defense), is completely dissonant with the content of the "Self-Serve Subscription Agreement" and the respective addendum relating to data processing (Data Processing Addendum version 3.0. - cf. evidence no. 66 of the Defense).

220. The allegation, in point 658 of the Defense, that "[was] based on the information provided by Cloudflare, Inc., namely in its Privacy Policy (cf. Policy attached as document No. 68), in Transparency Report (cf. Transparency Report which is attached as document No. 73) and in its Cloudsflare's commitment to GDPR compliance [...], that INE has withdrawn its conclusions about the US legislation and practices that may be applicable to Cloudflare, Inc . in the context of contracted services" could be considered if not for the fact that INE signed the contract in "February/March 2020" (cf. point 617 of the Defense) and the two documents invoked here are later, while Cloudsflare's commitment to GDPR compliance does not exclude, as shown, the application of US legislation.

221. And, therefore, in view of the content of the contract signed by INE, it is incomprehensible that he now claims, in point 682 of the Defense, that,"[...] according to his understanding based on the information he was given made available, these data were never in American territory, nor in the possession of the subcontractor". In effect, at this point of the Defense only a conviction of INE is invoked, not supported by facts, as demonstrated.

222. As for Defense's invocation of what it calls the European Data Protection Committee (CEPD) Guidelines - which correspond to Recommendation 01/2020 -, nothing in this document contradicts the CNPD's interpretation of the RGPD, which follows, to the letter, the judgment of the CJEU Schrems II, of 16

í

of July 2020, given that the CNPD never stated that there could be no flows of personal data to the US; he only reaffirmed that they depend on the adoption of complementary measures.

223. Furthermore, the CEPD document has a purely guiding nature, in the sense of supporting those responsible for the application of the RGPD, so the absence of these guidelines cannot justify the non-compliance with the obligations arising from that Regulation - moreover, these guidelines do not exist in relation to to other obligations that fall on the person responsible, and this does not mean that he is released from fulfilling them.

224. Regardless of the date of final approval of the aforementioned CEPD Recommendation 01/2020, the truth is that they were approved and made available for public consultation on 10 November 2020, so that, right there, INE had the opportunity to learn about the CEPD's recommendations on this matter, long before the census takes place.

225. The defense's prolonged allegation that, at the time Cloudflare, Inc. services were provided, the transfer of personal data was safeguarded by the European Commission's adequacy decision (Privacy Shield), which was only declared invalid by the Schrems II judgment of July 16, 2020, does not remove the obligation that falls on any person responsible for the processing of personal data to verify that the treatments they carry out comply with the conditions and limits provided for in the RGPD, being required of an entity such as INE, which processes personal data with special sensitivity and on a large scale, permanent attention to the legal framework of its processing.

226. In any case, the Schrems II judgment was published long before the 2021 Census operation was carried out (on July 16, 2020), with the Defendant having, however, the obligation to conform the processing of personal data designed with the said judgment , and had enough time to do so.

227. Incidentally, the contract with Cloudflare, Inc., which is alleged to have been entered into in February/March 2020 (cf. point 617 of the Defense) was entered into only for 11 (eleven) months, therefore, in effect, at best hypotheses until the end of February 2021. On the date of the eventual renewal of the contract, the judgment of the CJEU declaring the adequacy of the European Commission (Privacy Shield) invalid had already been handed down for more than seven months, therefore, both the parties are unaware of its content.

228. The Defendant further alleges that the contracted service ensured a set of technical measures capable of guaranteeing compliance with the RGPD (cf. point 677), namely: pseudonymization of personal data and encryption of information.

229. From the outset, the Defendant refers to Annex 2 of the Data Processing Addendum, not attaching said Annex, which contains the technical and organizational security measures to be adopted by Cloudflare, Inc., thus not demonstrating that they were relevant to the formation of the will to hire by INE.

230. Regardless, none of the measures invoked was actually applied in the contract signed by INE, nor could it be due to the nature of the contracted service (of CDN).

231. On the one hand, there was no pseudonymization of personal data.

232. On the other hand, regarding encryption, as will be better demonstrated in the next point, the service contracted by INE implied that Cloudflare, Inc., had the encryption key and decrypted the data packets.

233. The alleged considerations on data protection in the contracting of Cloudflare, Inc., were thus not demonstrated; on the contrary, what the facts demonstrate is a lack of care, not to say contempt, for the personal data protection regime and for the relevant jurisprudence in this matter.

234. In view of the above, the Defendant resorted to a subcontractor that does not provide sufficient guarantees for the execution of adequate technical and organizational measures to comply with the RGPD, at most its chapter V, which is clearly demonstrated by the clause of the contract, in violation of the obligation under Article 28 of the GDPR.

x. There were no data transfers to third countries

235. Following the explanation above, the Defendant sustains, in several points of the Defense (for example, points 531 et seq.), that the holders' data would never pass through servers other than those in Lisbon, this being the server that would be geographically located closest to the owner.

236. For what he considers impossible and impracticable, from a technical point of view, that data from the census operation Censos 2021 could have transited through servers located outside the European Union (cf. point 591 of Defense).

237. Lastly, the Defendant argues that the CNPD was unable to produce proof of any transfer of data to third countries.

analyzing,

Av. D. Carlos 1,134, Io

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

238. Firstly, it is clear from the Defense presented that the Defendant is unaware of whether the personal data of the holders, in response to the Census 2021 census operation, transited or not through servers of third countries.

239. Based on mere presumptions, the Defendant argues that this probability is very low, as there is a Cloudflare, Inc. server in Lisbon and, given the criterion of geographic proximity, that would be the one to be used.

240. The Defendant also assumes the hypothesis that the personal data, in the event of a "load" on the server, may have been in "mere transit" - an expression used in the Defense - on servers located in third countries.

241. The Defendant did not provide proof that he adopted the appropriate guarantees, within the scope of the Census 2021 census operation, in accordance with Chapter V of the RGPD, as was required of him, having therefore violated article 44 of the RGPD.

Otherwise, let's see,

242. Firstly, it is clarified that the CNPD never questioned that "personal data and other information collected within the scope of the response to the 2021 Census via the internet [...] were always [...] housed in the systems and infrastructure from INE itself [...]" (cf. points 527 and 528 of Defense). What was always at stake was the transit of personal data.

243. The use of a CDN aims to reduce the latency of invocations to websites, reducing loading time. A web page can be made up of a set of resources that are requested by the client from the server when rendering17 the page on the browser screen (or another type of application used to access HTML pages available online). The more resources needed (e.g. images, style files,

code files, video and/or audio files), and the longer it takes to download them to the client machine, the longer the graphical presentation of the page will take to complete.

244. Considering the majority of websites, the time it takes for the page to be displayed to the visitor/user depends, to a large extent, on the delay in delivering these resources when requested (on the browser-Internet browser side) to the server, and then sent from back from the server to the browser. Since Internet communications are materialized by electrical circuits with electronic components such as "routers" along the way, the transit time is very dependent on the number of

17 Process of interpreting the HTML, CSS and javascript code, along with the inclusion of content such as images, videos, or audio, in the production of web pages in the client application (browser).

W... _"

National Data Protection Commission

hops (/iops18) that packets of information have to go through when being "routed19" from one point to another. The greater the geographic distance between the nodes, the greater the probability that the number of forwarders will increase, and thus also the greater the time it takes the packet to go from source to destination.

245. The use of CDNs is intended to reduce page loading time, acting precisely on this transmission time, as explained below.

246. Resources or content can be divided into two types: static and dynamic. Static contents (eg, images, audio, video, CSS style files, files with JavaScript code) do not vary and are always the same, remaining unchanged for any invocation. Dynamic contents (e.g., HTML pages, in this case, forms) are processed in each request, and may produce a different result each time; may vary, for example, depending on the parameters sent in the request to the server (e.g., querystring, POST parameters, cookies).

247. In this way, static content can be cached and reused again and again without becoming out of date, without causing any damage to the user experience. The same does not happen with dynamic contents, which have to be processed at each invocation.

248. CDNs intend to reduce loading times and, for this purpose, make static contents available more quickly, keeping them in cache. Since these contents do not change, after the first request has been served, the remaining requests can reuse the

content that was stored locally, without having to request it again from the server where the website resides.

249. For this to happen, traffic from the client (browser) to the server is directed to a content provision network (in this case, the CDN), made up of several machines connected to each other. If the request that arrives at one of these machines, possibly the one geographically closest to the client, is for static content, and if it had previously been stored in that machine's cache, the CDN no longer forwards the request to the server and serves the resource directly to the client (browser), significantly reducing the response time.

250. As for requests for dynamic content, this cannot be done. Once the request arrives at one of these machines, it is forwarded to the server that awarded the CDN service (in this case, the

18 The logical measure of the size of a network can be counted in the number of hops, that is, the number of routers that a packet has to go through to go from source to destination.

19 Routing is the process of forwarding information packets on IP networks, directing traffic from router to router from source to destination.

INE) and processed with each invocation, thus, due to its nature, it cannot be stored and reused for future requests.

251. As is understood, the CDN machines only keep static content stored, since the dynamic ones would be of no use to them because they cannot be reused.

252. In the aforementioned paragraph 469 of the Defense, later reaffirmed in paragraph 479, the Defendant alleges that "the dynamic contents of the 2021 Census website - more specifically, the specific electronic form for collecting the questionnaire

[...] which contained personal data of the citizens [...] were never hosted in Cloudflare's cache, nor was it demonstrated that their traffic was carried out through the CLoudflare CDN [...]".

253. The first part of the claim is correct, given that the CNPD never claimed that dynamic content was cached. In fact, to make a CDN useful, only static resources need to be cached.

254. The second part of the aforementioned statement, which states that the transit of requests for dynamic content, and the respective responses, through the CDN of Cloudflare, Inc., has not been demonstrated, is not true, as demonstrated by the evidence collected by the CNPD, relating to the traffic of requests for dynamic content, with responses to the Specific Electronic Form (FEE), by the servers of Cloudlflare, Inc.

255. To verify this fact, the CNPD carried out several surveys, which focused on the functioning of the form available at censos2021 .ine.pt. The form was tested and the respective sessions were recorded, extracting images that demonstrate the opposite of what was stated by the Defendant in the Defense (cf. Annexes to the document Info UI AVG 2021 401 II vl.O.docx, "Screen captures showing the data packets exchanged between the client and the servers (Tine.pt), while completing the 2021 Census form", pages 29 and 30).

256. Indeed, when accessing the 2021 Census questionnaire online, available at censos2021.ine.pt, the user was prompted to enter the code and password contained in the letter he received at his residence. Submission of the form would send this data back to the address censos2021.ine.pt, as shown in the images of the session maintained between the browser and the server (cf. Attachments to the document Info UI AVG 2021 401 II v1.0.docx, "Capturas de screen showing the data packets exchanged between the client and the servers (Tine.pt), while completing the 2021 Census form", pages 29 and 30).

257. After completing, in the online form, the answers to the questions that made up the 2021 Census questionnaire, which collected personal data, the data was sent to another web server at the address fee.ine.pt, as can also be done see in the images of the session (cf. Attachments to the document

Info UI AVG 2021 401 II v1.0.docx, "Screen captures showing the data packets exchanged between the client and the servers

(*.ine.pt), while completing the 2021 Census form", page 29 and 30). This server implemented the FEE whose purpose was to collect data from respondents.

258. Both the censos2021.ine.pt and fee.ine.pt websites were being, until April 26, 2021, resolved to IPs assigned to Cloudflare, Inc., as attested by the DNS20 lookup queries carried out during the expertise, some of which were collected as evidence (cf. Attachments to document Info UI AVG 2021 401 II v1.0.docx, “Resolution of domain names, IP lookup, reverse DNS, routing", pages 22 to 28).

259. It is thus proven that requests for both static and dynamic resources (the latter containing personal data of census respondents) were being forwarded to the machines under the responsibility of Cloudflare, Inc.

260. As stated in paragraph 470 of the Defense, that personal data would not be forwarded to Cloudflare, Inc. servers, is not true.

261. It should be added, for better clarification, that what the CNPD presents, in the information dated September 16, 2021, is a scenario of compliance for the use of the CDN, which involved the submission of requests for dynamic content to be made directly to the INE server in Lisbon; simply, in the concrete case, this scenario did not happen.

262. Therefore, the conclusion advanced in point 482 of the Defense is also unfounded. In technical terms, as the CNPD well explained in that information, the use of CDNs was never in crisis, but the way in which the online collection of data from the 2021 Census was carried out. It is technically possible, and even so advantageous in terms of performance and security, to maintain the use of the CDN for storage and availability of static resources, and the submission of data can and should be done directly to the final server of the controller.

263. And what is stated in point 552 of the Defense is also inaccurate, where it says "[...] on the contrary, the personal data and other information collected in the context of the response to the 2021 Census via the internet [...] were directly directed to INE's data center".

264. In the "Communiqué from Cloudflare of 04-05-2021" (according to point 537 of the Defense), the company assumes that "[...] Portuguese citizens seeking to provide Information to INE for the census would have been directed to 20

20 Domam Name Server is the designation for the servers whose function is to "translate" a "name" like www.cnpd.pt into an IP address. For communication between two machines to be possible, the information packets need to carry the addresses IP of both.

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

INE's website through the Cloudflare data center closest to the user, scanned for malicious code or activity as directed by INE, and sent directly to INE's hosting servers

265. This statement is in line with the analysis and conclusions of the CNPD on the process of forwarding information from the client to the server and contradicts the Defense's argument that requests for the dynamic contents of the website, which include the participants' responses to the questionnaire , would not be being forwarded by Cloudflare, Inc.'s CDN.

266. As Cloudflare, Inc. itself admits, the participants' responses would be forwarded to the data center closest to the user (which for citizens filling out the questionnaire in Portugal allegedly would be the data center in Lisbon) and analyzed to detect malicious activities or code [through the WAF (Web Application Firewall) service, subscribed by INE to Cloudflare, Inc.], and only then sent to INE's servers, according to INE's instructions, which, therefore, could not unaware of this fact - contrary to what he is now claiming.

267. The communication from Cloudflare, Inc., contradicts the claim that the sending of personal data collected in the online questionnaire would not pass through the servers of Cloudflare, Inc., being forwarded directly to the server of INE.

268. It is important to clarify that any of the services provided, CDN or WAF, oblige the Cloudflare, Inc. machines, which receive the requests, to have access to the information package data in order to know the destination they are going to give them. If in the case of the CDN the package is opened to determine if the requested resource is static and if it is in the cache, in the case of the WAF the package is opened to verify the possibility of attack, such as injection of malicious code.

269. Just as what was written in point 553 of the Defense is also not true. The evidence taken from the investigations carried out support that from the beginning of the online questionnaire collection operation until the end of the day of the CNPD inspection of INE, either the address censos2021.ine.pt, where the user is asked to introduce personal data such as code assigned to your home and respective password, and the address fee.ine.pt, where data from the answers to the 2021 Census questionnaire would be submitted, were being resolved to IP addresses assigned to Cloudflare, Inc., which would lead for traffic to those addresses to be forwarded to machines under that company's control.

270. In points 558 to 561 of Defense, it is admitted that the WAF service, subscribed by INE to Cloudflare, Inc., subjects the information packets to the analysis of "specific elements associated with the communicated information". In order to collect information from respondents, they "[...] enter their responses in the FEE application [...] available on the same website [censos2021.ine.pt and fee.ine.pt]" , and then "the

data (personal and non-personal) contained in these responses must be transmitted to the data center of INE". In order to prevent these attacks [...] the WAF acts as [...] [a] shield placed between the user and the server, in such a way that network traffic (namely, responses entered by citizens in the FEE) must first pass through this firewall before reaching the INE server.".

271. It follows that the information packets with personal data are opened and inspected by the WAF service of Cloudflare, Inc., which turns out to be recognized by the Defense, in clear contradiction with what was previously alleged.

272. Indeed, in paragraph 562 of the Defense, the Defendant states that this operation is carried out "without accessing the content of the transmitted information", which would be a contradiction and obviously does not correspond to the truth. In fact, all packages are open and for the analysis of the content to be done "automatically", the WAF will focus on the elements that appear in the body of the request. These elements include the data entry fields on the survey pages with the values filled in by respondents. By analyzing the body of the request, the WAF has access to all the information entered by the respondent in the fields at its disposal.

273. Again, Defense point 564 is untrue. Here it is said that "the WAF does not access the content of the information in traffic,

and there is no [...] any possibility of accessing or consulting the personal data contained in the responses transmitted to the INE server". other allegations of the Defense, specifically in point 561, where it is said that "the Cloudflare firewall analyzes specific elements associated with the communication that may indicate attacks [...]".

274. At the same time, point 569 of the Defense is, for the same reasons, false. Here it says that "[in] the use of the three Cloudflare services [WAF, CDN, Rate Limit], there was no access or transmission to Cloudflare at any time of the responses entered by the respondents, namely the responses entered by them in the FEE available on the website «CENSOS2021 .INE.PT»", it being redundant to refute this statement, given the exhaustive explanation already left here.

275. As for the alleged impossibility and impracticability, from a technical point of view, of the data coming from the census operation Censos 2021 having transited through servers located outside the European Union (cf. point 591 of the Defense), it is important to compare the content of the communiqué of Cloudflare, Inc., with the Defense allegations, to reach the opposite conclusion.

Av. D. Carlos 1,134,1o

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

276. Although Cloudflare, Inc., has registered IPs in the European Union, the IPs for which the censos2021.ine.pt address resolves are registered in the USA - 104.22.20.250 and 104.22.21.250 (cf. https://bgpview. io/asn/13335#prefixes-v4).

277. The fact that the servers are using IPs from Cloudflare, Inc., registered in the USA, when the company has IPs registered in the territory of the European Union, is in itself demonstrative that care was not taken to ensure that personal data would only circulate within the territory of the Union.

278. Incidentally, proof that Cloudflare, Inc., transmitted and transmitted personal data to the US even in the contracts that guaranteed customers the restricted access service by geographic area (Cloudflare Data Localization Suite) can be easily found in company's Internet site, in the information provided. There, at the time of the facts, it was reported that:

"Regional Services. Cloudflare has data centers in over 200 cities across 100+ countries. Regional Services together with our Geo Key Manager solution allows Customers to pick the data center locations where TLS keys are stored and TLS termination takes place. Traffic is ingested globally, applying L3/L4 DDoS mitigations, while security, performance, and reliability functions (such as, WAF, CDN, DDoS mitigation, etc.) are serviced at designated Cloudflare data centers only.With Regional Services, some metadata will still be transmitted to our core data center in Portland, Oregon. However, the only Personal Data we collect in these logs are IP addresses. [.../" (emphasis added) - cf. https://web.archive.Org/web/20210426141842/https://www.cloudflare.com/adpr/introduction/21

279. That is, the metadata, which includes the respondents' IP22 personal data, collected by Cloudflare, Inc. in the audit logs, were transmitted to the US.

280. It is also significant that, however, the information made available on that site has changed, no longer stating that the metadata is transmitted to the US (cf. https://www.cloudflare.com/gdpr/introduction/), the which occurred, perhaps, following the CNPD's draft decision and also other draft decisions from other supervisory authorities of Member States of the European Union.

281. It is also true that the services provided by Cloudflare, Inc., namely those contracted by INE when it subscribed to the Business Plan, place the company directly under the purview of US legislation, which imposes on it the obligation to grant mass access to data personal data handled by you, provided

21 To access the information on the Cloudflare, Inc. website, on April 26, 2021, on the date of approval of this determination, the WayBack Machine's Internet page history was used.

22 Cf. Judgment of the CJUE in Process C-582/14, August 19, 2016,

therefore as a provider of electronic communications services23, without prejudice to other types of services being equally covered by other provisions of the US legislation on surveillance and national security.

282. Cloudflare, Inc., recognizes in point 7 of the Data Processing Addendum version 3.0 that, in its role as a data processor, it

may be subject to requests for access to personal data by third parties within the scope of legal procedures, which may be "inconsistent" with the law applicable to your customer, i.e. the GDPR. In this case, where there is a conflict of laws, Cloudflare, Inc. declares that it will immediately inform the customer, «unless such notification is legally prohibited» (cf. paragraph a) clause 7.1)24.

283. It is precisely the case of this US legislation that prevents US companies from informing their customers of access carried out by US authorities for the purpose of collecting information on foreigners, in the context of national security activity.

284. In view of these facts, the person responsible was not able to demonstrate, as required by Article 5(2) and Article 24(1) of the RGPD, that it applied the appropriate measures to ensure and be able to prove that the processing of personal data was carried out in accordance with the GDPR, in particular Article 44 of the GDPR.

285. It is also important to emphasize that the Defendant, also in what he considers to be valid arguments for his Defence, again shows the weaknesses in monitoring the regulatory changes operated with the entry into force of the RGPD, from the outset, when he insists that the mere transit of personal data by third countries is not legally relevant today.

286. In fact, Article 4(1)(c) of Directive EC/95/46 of 24 October 1995, as well as Article 4(3)(c) of Law No. 67/98, of October 26, which transposed the Directive, excluded from the scope of application of the data protection legislation, if the person responsible was not established in the national territory, the processing of personal data when the means were used for transit.

23 FISA Section 702 as amended by 50 USC § 1881a.

24'[.../ If Cloudflare becomes aware of any third party legal process requesting Personal Data that Cloudflare processes on behalf of Customer in its role as data processor or sub-processor (as applicable) then, to the extent that Cloudflare is able to identify that such third party legal process requesting Personal Data raises a conflict of law, Cloudflare will: (a) immediately notify Customer of the request unless such notification is legally prohibited;

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

287. However, this provision was not included in the RGPD, and therefore the transit of personal data was not excluded from its objective scope of application, given that it corresponds to an operation involving personal data, under the terms of paragraph 2) of article 4 of the GDPR.

288. Incidentally, in paragraphs 602 et seq. of the Defence, the invocation of CJEU jurisprudence to substantiate that the operation of transmitting personal data to third countries would not fall within the objective scope of application of the current legal regime of data protection is, strangely enough, , reduced to a judgment from 2003, which is identified as "[...] one of the only cases decided by the CJEU on restrictions on data transfers to third countries [...]" (cf. point 602 et seq. of Defense), when it is true that there is numerous jurisprudence of this Court on the transmission of personal data to third countries, part of which already considering the RGPD - Judgment Maximillian Schrems c. Data Protection Commissioner (Schrems /), proc. C-362/14, of October 6, 2015, the judgment Data Protection Commissioner c. Facebook Ireland Ltd and Maximillian Schrems (Schrems II), proc. C- 311/18, of July 16, 2020, and the TJEU Opinion 1/15, of July 26, 2017, on the PNR agreement between Canada and the EU,

289. It is also true that there is no parallel, nor basis for analogy, between the case examined in that judgment referred to by the Defense and the case analyzed here.

290. On the other hand, what is stated in paragraphs 610 et seq. of the Defense is irrelevant to the present case, since the aforementioned position of the UK supervisory authority is based on the assumption, made explicit in the aforementioned citation, that there is no access or manipulation of personal data when they arrive at a server located in the territory of a third country. However, the CNPD has already demonstrated that the services of Cloudflare, Inc., contracted by the Defendant require the opening and verification of the information packets, so that position is, in this context, irrelevant.

291. Regarding the invocation of the document of the European Committee for Data Protection (CEPD) that the Defendant identifies as "Guidelines 1/2020" - rectius, Recommendations 1/2020 on complementary measures to the transfer instruments to ensure compliance with the level of protection of EU personal data - nothing in this document contradicts the CNPD's

interpretation of the RGPD, which strictly follows the TJUE Schrems II ruling of July 16, 2020, given that the CNPD never stated there can be no flows of personal data to the US; he only reaffirmed that they depend on the adoption of complementary measures.

292. Furthermore, the CEPD document is merely a guideline, and the person responsible is not exempt from complying with the obligations arising from the RGPD as long as there are no guidelines or recommendations from that body.

. D

National Data Protection Commission

293. Regardless of the date of final approval of the aforementioned CEPD Recommendations 1/2020, the truth is that they were approved and made available for public consultation on 10 November 2020, so that, right there, INE had the opportunity to learn about the CEPD's recommendations on this matter, convening, at this venue, what was said above, in points 223 to 225 of this Resolution.

294. In summary, the Defendant did not apply the appropriate measures to ensure and to be able to prove that the processing of personal data was carried out in accordance with the RGPD, in particular, with article 44 and paragraph 2 of article 46 .° of the RGPD, but the CNPD considers that the breach of the obligation to adopt appropriate security measures provided for in article 32 of the RGPD has been consumed in this infraction.

xi. About the mandatory Impact Assessment on Personal Data

295. The Defendant alleges that in the 2021 Census statistical operation the Impact Assessment on Personal Data (AIPD) may be waived.

296. Namely when there is a pre-existing AIPD already carried out for a previous identical statistical operation.

297. In the opinion of the Defendant, this is what happens, sn casu, insofar as he has an authorization issued by the CNPD under the terms of Law No. 67/98, of October 26, specifically Authorization No. 2600/2011 , which refers precisely to the General Population and Housing Census operation.

298. Authorization No. 2600/2011 has never been amended, replaced or revoked.

299. Therefore, in the Defendant's opinion, he was exempt from drawing up an AIPD prior to the processing of personal data.

300. Also because, in his opinion, the only change verified, from the 2011 Census census operation to the 2021 Census census operation, involved adopting risk mitigation measures.

301. The Defendant argues that the very concept of an AIPD cannot necessarily mean that it is definitively formalized and reduced to writing even before the start of the processing operation.

302. The Defendant did not postpone or fail to carry out an AIPD prior to the beginning of the census operation.

303. It only proceeded diligently, in seeking to ensure its improvement and updating throughout the 2021 Census process.

v.

/

304. The Defendant also argues that, before the performance of an AIPD can be definitively concluded, it must be progressively updated - which the Defendant did, despite the fact that such AIPD is not required of him.

305. Therefore, it cannot be considered that the Defendant carried out the AIPD at a late time, but rather it must be considered that the Defendant diligently fulfilled an obligation that was not applicable to him.

306. Only in the context of the main census operation Census 2021 was it possible, due to the pandemic context and health emergency, to definitively decide on the collection processes and application functionalities used, so that, only at that moment was it justified to carry out the AIPD.

307. This does not justify any insufficiency of the AIPD, being only the result of the context of constant uncertainty experienced due to the Covid-19 pandemic.

308. The Defendant further alleges that the fact that the main census operation Census 2021 encompasses, in itself, different operations for processing personal data, does not mean that all these operations involve such a risk and that they all require an AIPD.

309. With the exception of the operation of collecting and processing data from respondents to the "2021 Census" questionnaire - duly reflected in the AIPD carried out - there appears to be no other data operation carried out that constitutes

any risk for the holders of personal data.

310. Therefore, the AIPD carried out is not insufficient.

311. It also adds on the AIPD that it punctually complied with the minimum content to which it was bound under the terms of paragraph 7 of article 35 of the RGPD.

Let's see,

312. It should be noted, from the outset, that CNPD Authorization No. 2600/2011 had as its object the processing of personal data carried out in a temporally delimited census operation - year 2011 -, which is why that authorization has exhausted its effects, or if you prefer, it expired, ipso iure, with the end of the said operation.

313. Furthermore, the authorization was valid specifically for the 2011 census operation and in accordance with the elements notified by INE to the CNPD at the time, so that, due to the changes produced in the 2021 census operation compared to 2011, always would have to be concluded by the expiry of that authorization.

314. Namely, that authorization does not include any reference to the collection of responses to surveys via the Internet, nor to the transfer of personal data to third countries - which, as seen above, should be analyzed and mitigated, as it does not even mention the existence of any subcontractor, very least headquartered in a third country, all novelties introduced in the processing of personal data carried out in the 2021 census operation, which increase the risks to the rights of the holders.

315. Furthermore, the Defendant himself acknowledges, with regard to the 2021 Census operation, the need to adopt "(■••) a new census model in 2021", a model that "(...) is based, in whole or in part, on the use of administrative information", (cf. points 56 and 57 of the Defence).

316. Indeed, "[the] transition to an administratively based census model would therefore have in view (...) the reinforcement of the integration of census data in the INE's statistical information system on families (.. .)" (cf. point 58 of the Defense).

317. From which it can be seen that, clearly, the conditions under which the 2011 census took place are not identical to the 2021 census operations, so that the authorization would always have to be considered as expired.

318. And an expired administrative act does not produce legal effects for the future, and therefore cannot be subject to revocation or replacement, as results from paragraph 2 of article 166 and paragraph 1 of article 173 of the Code of Administrative Procedure, so the Defendant could never have the expectation that the non-revision of the authorization by the CNPD would mean the confirmation or extension of its content for the 2021 census operation.

319. Incidentally, the fact that each census operation is regulated specifically and autonomously by its own legal diploma - see Decree-Law no. 226/2009, of September 14, and Decree-law no. 54/ 2019, of April 18 -, demonstrates that each census operation implies an autonomous and distinct processing of personal data, therefore having a specific legislative framework.

320. Moreover, this conclusion is reinforced by the fact that Decree-Law No. 54/2019 does not even have to revoke Decree-Law No. 226/2009, just as this diploma did not revoke the Decree-Law on 2001 census.

321. It cannot, therefore, be claimed that the processing of personal data arising from the 2021 census operation is the same, or even equivalent, to that carried out in the context of the 2011 Censuses.

322. Reasons why the arguments of the Defendant, contained in points 710 to 745 of the Defense, on the use of the content of Authorization No. 2600/2011 in the context of the operation

census 2021 to claim to be exempt from an obligation provided for in the RGPD and applicable to it since May 25, 2018.

323. Furthermore, the Defendant was obliged to carry out the AIPD, under the terms set out in paragraph 1 and paragraph b) of paragraph 3 of article 35 of the RGPD, it being clear that the 2021 census operation involved the collection and subsequent processing on a large scale (the entire population residing in the national territory) of special personal data, more specifically, data relating to religion and health.

324. It is also important to remember that the AIPD corresponds to a joint assessment of the processing of personal data, so it should not be restricted only to the conditions for processing special data, leaving out the processing of other personal data.

325. Incidentally, Regulation No. 798/2018, of November 14, on the list of personal data processing subject to an Impact Assessment on Data Protection, approved by the CNPD under Article 35(4) .° and subparagraph k) of paragraph 1 of article 57, both of the RGPD, provides in paragraph 2 the obligation to carry out an AIPD when in question is a «[...] processing that relates personal data provided for in article 9(1) or in article 10 of the RGPD or data of a highly personal nature", as clearly happens in the 2021 Census.

326. In fact, in addition to the Defendant collecting personal data that fall into the category of special data, provided for in paragraph 1 of article 9 of the RGPD, he also collects personal data that reveal private and family life, in his stronghold more intimate part of daily life, corresponding to the category of data of a highly personal nature that the Article 29 Working Group highlights in order to consider them a criterion that fits under Article 35(1) of the RGPD (cf. point 4. of the Guidelines relating to the Data Protection Impact Assessment and determining whether the processing is «likely to result in a high risk» for the purposes of Regulation (EU) 2016/679 - WP248 rev.01, revised and adopted on 4 October 2017), which was assumed by CEPD on May 25, 2018.

327. Criterion that is also set out in no. 2 of Regulation no. 798/2018, of 30 November, on the list of personal data processing subject to an Impact Assessment on Data Protection.

328. Therefore, the obligation to carry out the AIPD is not restricted to formally special or sensitive personal data, and should extend to all personal data subject to processing in the 2021 Census operation, also because the processing of personal data, as defined in paragraph 2 of article 4 of the RGPD, comprises the entirety of the operations carried out on personal data in the context of a given activity or operation.

329. As for the relevant moment for carrying out a DPIA, it is clear that it must be prior to the start of the processing of personal data, as is explicitly established in paragraph 1 of article 35 of the RGPD («[...] the controller carries out, before initiating the processing, an impact assessment on the protection of personal data. [...]» (emphasis added), and also in recital 90 of the RGPD, regardless of whether to be subsequently revised according to the needs

330.Now, on April 26, 2021, during the inspection, the CNPD asked the Defendant for the AIPD, the corresponding opinion of the data protection officer (EPD), a copy of the contract signed with the company hired to, on a technical level, develop the form for collecting and further processing personal data associated with the 2021 Census (AGAP2IP) and a copy of the Audit Report prepared by the National Security Office.

331. That same day, at 9:00 pm, the Defendant sent the aforementioned elements to the CNPD, by email, with the exception of the AIPD and the Opinion of the EPD.

332. On May 27, 2021, the CNPD insisted on sending the missing elements, which were only received on June 28, 2021.

333. The document designated AIPD is not dated, indicating only the year.

334. However, it is INE itself that assumes that it has not formalized the AIPD, although it claims to have gathered the "materially characterizing elements of an AIPD, such as the risk assessment of the assets involved in the various treatments carried out, which is integrated in the present AiPD and which was revised in 2020 and 2021 (before the beginning of the census operation)".

335. Thus, documentation was not delivered to the CNPD demonstrating that a previous and complete AIPD had been carried out before the start of data processing to be carried out within the scope of the 2021 Census operation.

336. In addition, the document sent to the CNPD under the title "Opinion on the Impact Assessment on Data Protection of the 2021 Census statistical operation" of the EPD, is dated May 12, 2021, that is, the date after the start the performance of the census operation and subsequent inspection by the CNPD.

337. Annex 20 to the AIPD, without identification, but recorded as “Treatment of risks", indicates, as the date of the last update, May 3, 2021. Strangely, no version of the document with an earlier date was presented, nor with date prior to the start of the census operation. Furthermore, it is inexplicable that an updated version of the risks is made in May 2021 while maintaining the data protection risks related to the data processing operation that had already been suspended on April 26,

í

2021 by INE, following inspection by the CNPD and before formal knowledge of the suspension order.

338. Notwithstanding the said annex not complying with the rule of article 54 of the Code of Administrative Procedure, according to which "the language of the procedure is Portuguese", a rule that INE does not follow with regard to a document drawn up , apparently by their own services and marked at the top as "Internal use - Internal use", this document does not support a risk analysis prior to initiation of treatment.

339. Not even the few references to the document, in the so-called AIPD, in three short paragraphs, on pages 46 and 47, demonstrate the effective assessment of these risks or the adequacy of measures to mitigate them.

340. Now, it is clear that an AIPD must be documented, and when it is mandatory, an AIPD that is only "in the head" of the person responsible for the treatment is of no use.

341. That follows from several provisions of Article 35 of the GDPR, which presuppose such documentation. As an example, consider the minimum content of an AIPD, specified in paragraph 7 of the aforementioned article - firstly, the requirement for a systematic description of the planned processing operations or even the request for the opinion of the person in charge of data protection data imposed by paragraph 2 of the same article.

342. And it also follows from the joint reading of article 35 of the RGPD with the principle of responsibility, enshrined in paragraph 2 of article 5 of the same diploma, which determines that the person responsible must be able to prove that he complies with the principles of data protection, here directly emphasizing the principles of lawfulness, loyalty and transparency, minimization of data and integrity and confidentiality, either with paragraph 1 of article 24, all of the RGPD, which provides for the duty to adopt [...] the technical and organizational measures that are appropriate to ensure and be able to prove that the treatment is carried out in accordance with this Regulation'.

343. Proof of compliance with the RGPD, whether specific obligations or data protection principles, implies that the person responsible has elements that demonstrate such compliance, which in the case of the obligation to carry out an AIPD depends on any process documented, whatever its support (e.g., paper, digital). It is not, therefore, a matter of demanding the "formalization" of the AIPD, but rather the obligation provided for in article 35 of the RGPD assumes any materialization of the same, which allows demonstrating its implementation, which the Defendant was manifestly unable to to do, neither when requested by the CNPD nor during a prior hearing in this procedure. Nor is it discussed that an AIPD represents a continuous

process (cf. point 767 of Defense). There is no apparent legal basis for the

Defendant considers that, at the start of the census operation, the existence of comprehensive and complete documentation on the AIPD, with the elements available, was not required.

344. Furthermore, the argument that the IAPD should be dynamic, subject to revisions and updates whenever necessary, obviously does not affect the duty to document the assessment already carried out before the moment of that revision or update.

345. Furthermore, in his Defence, the Defendant does not demonstrate that he actually carried out any AIPD before the start of the operation, nor a full assessment of the risk of transferring personal data to third countries.

346. Furthermore, the document called AIPD is not complete, since it only refers to four data processing, namely: "Processing 1 (TI) Data necessary for contact with the household representative (data taken from the National Data File Accommodation)"; "Treatment 2 (T2) Respondent data (statistical data provided by respondents when completing the Census form, regardless of the means of transmission of the informationl)"; "Treatment 3 (T3) Data from subcontractors involved in Census activities"; "Treatment 4 (T4) Resident Population Base (BPR) - Only to reinforce the quality of the census results, in the statistical treatment phase, and, within the scope of the contingency plan resulting from the COVID 19 pandemic, allow imputations in case response;

347. It should also be noted and emphasized that the pandemic period experienced did not suspend the obligations resulting from the RGPD for those responsible for processing personal data and, in particular, did not suspend the duties and obligations imposed on administrative entities.

348. Therefore, it can only be considered that the Defendant confirms, with his Defence, the failure to carry out an AIPD, confirming the non-compliance with the provisions of article 35 of the RGPD.

xii. Lack of communication from the EPD

349. The Defendant alleges that he communicated the contact details of his EPD to the CNPD.

350. On 22.05.2018, the Secretariat of the INE's Board of Directors sent, to the email address geral@cnpd.pt, a communication informing that the graduate in law Ana Dulce Pinto, Higher Technical Specialist in Statistics at INE, had been designated in charge of data protection at INE, as of 25 May 2018.

Av. D. Carlos 1,134,1o
1200-651 Lisbon
T(+351) 213 928400
F (+351) 213 976 832
geral@cnpd.pt
www.cnpd.pt

v.

r

351. On 19.05.2021, INE's Board of Directors decided to renew the mandate of Dr. Ana Dulce Pinto in the role of EPD at INE, for the 2021/2023 period.

Let's see,

352. It should be noted that the Defendant provided sufficient proof of the practice of the obligations resulting from the provisions of paragraphs 1 and 7 of article 37 of the RGPD.

353. Namely by attaching an e-mail to the present case file.

354. This is why the CNPD understands that the infringement for which it was accused has not been verified.

xiii. Waiver of fine, pursuant to 44th paragraph 2 of Law 58/2019

355. The Defendant considers that the specificity of the processing of personal data carried out in the context of the Census 2021 census operation does not raise particular needs for general or special prevention, which oppose the waiver of a fine, pursuant to the provisions of paragraph 2 of article 44 of the LERGPD.

Let's see if such a regime can be applied to the Defendant,

356. The mechanism provided for in paragraph 2 of article 44, now requested by the Defendant, does not constitute any

rule-principle waiving the application of fines to public entities.

357. Nor could it be, under penalty of seriously contravening the provisions of paragraph 1 of the same article 44.

358. In fact, the national legislator, via Article 44(2), created a mechanism that can only be used by public entities.

359. This mechanism is not the general rule, as it is contained in Article 44(1), which provides for the imposition of fines on public and private entities alike.

360. Paragraph 2 of that article represents only an exceptional regime for public entities.

361. Which is still dependent on a "duly substantiated request" to the Control Authority.

362. What, incidentally, was clarified in Deliberation/2019/945 issued by the CNPD, which made explicit that the waiver of the imposition of fines on public entities depends, under the terms of paragraph 2 of article 44 of the LERGPD , of a discretionary assessment (or autonomous, in the sense of not predetermined by law) by the CNPD of the grounds invoked by the applicant.

363. Now, in the case of the Defendant, it should be noted that we are facing a high number of administrative offenses, practiced within the scope of the same census operation Census 2021.

364. On the other hand, we are facing a mass data processing operation, that is, the universe of affected personal data holders is very wide (the entire population in Portugal in terms of general data processing, and more than 6 million people regarding international data transfers).

365. In addition, some of the infringements concern the processing of data specially protected by the GDPR.

366. It should also be noted that the Defendant was charged with several violations of the provisions of the RGPD, which are classified as serious and punishable by the highest penalty, provided for in the RGPD.

367. All in all, it is concluded that there are weighty reasons for imposing a fine on the Defendant, with no exceptional circumstances that deserve consideration for the purpose of its non-application.

368. In view of the lack or insufficiency of grounds for the application and considering the nature and extent of the processing of personal data, as well as the seriousness of the infractions, the CNPD rejects the request for waiver of the fine made by the

Defendant.

III. Facts

369. Of the elements contained in the file, of interest for the decision, the factuality contained in the Draft Deliberation is deemed to be partially reproduced.

370. It should, however, be mentioned that it is considered proven, contrary to what is contained in the Draft Deliberation, that the Defendant published his EPD data and communicated them via email to the CNPD.

371. Therefore, the following facts are considered as proven and of interest for this Deliberation:

i. Between April 19 and May 31, 2021, the census operation "2021 Census" took place

ii. It aimed to obtain information about the entire population residing in Portugal, families and the Portuguese housing stock;

iii. The response to the 2021 Census by the holders of personal data was mandatory and the failure to provide information or the provision of inaccurate information punishable with a fine between €500 and €25,000;

v.

*■ r

iv. By April 26, 2021, the date on which the CNPD began investigations, around 2.5 million forms had been submitted online;

v. Which covered the processing of personal data of more than 6 million people;

saw. INE, as the national statistical authority responsible for processing personal data, organized the entire census procedure;

vii. By option of INE, the processing of information by digital means was privileged, to the detriment of filling in and delivering physical forms;

viii. Between April 17 and May 7, 2021, a large number of complaints related to the census operation Census 2021 were filed with the CNPD;

ix. The complaints filed relate to four aspects:

The. The legality of the processing of personal data that explicitly identified their holders by name;

B. The legality of collecting special categories of data, such as those relating to religion, emphasizing the apparently mandatory nature of the response;

w. The security of the information handled; It is

d. The existence of international flows to countries that may not ensure an adequate level of protection of processed personal data, compatible with European legislation;

x. Within the framework of the powers conferred on it by law, the CNPD carried out the inspection process, having visited, on April 26, the premises of the INE headquarters, for this purpose.

And still

i. Lack of legal basis for the processing of special categories of personal data

372. In the forms presented to data subjects, in order to comply with the obligation to respond to the 2021 Census (items 29.1 to 30), personal data of special categories were required.

373. Namely, data relating to health problems and religion of respondents.

374. Respondents were asked about special categories of data in the items of block 3 "Individual" (cf. printing of the online census form with the process):

The. 20 ("He did not work from the 12th to the 18th of April because: (...) He is permanently unable to work");

B. 29 (relating to the physical difficulties of the respondents); It is

w. 30 ("Indicate your religion").

375. The forms were not clear in delimiting the information to be provided versus the optional information.

376. There was no information that the answer to questions 29.3 to 29.6 and 30 was optional.

377. The questions in group 29. consisted of 6 questions, framed in 3 pages, with two questions in each of them.

378. Only the first page had information about the optional character.

379. On the next two pages (questions 29.3 to 29.6), the optional nature of the answer was not informed.

380. Item 30., although optional, did not provide any information.

ii. Violation of the duties of informing data subjects

381. INE did not make available on the Census page, nor on the forms, an obvious, highlighted and easily accessible information where the data subject could know, with the necessary detail, the circumstances in which the processing of his personal data would occur, or even hyperlink on that topic that referred to another page, where such information was provided.

382. Nor was this information about this processing of personal data available on the institutional website of INE,

iii. Violation of the rules applicable to the employment of Cloudflare, Inc.

383. The contracting of Cloudflare, Inc., did not deserve any negotiation or prior "due diligence" by INE.

384. INE limited itself to subscribing online to the services provided, in a package, by Cloudflare, Inc.

385. INE opted to subscribe to the "Business" package with Cloudflare, Inc., headquartered in the USA.

386. The "Business" package was, at the time, governed by the "Self-Serve Subscription Agreement", and by the addendum relating to the processing of personal data (Data Processing Addendum version 3.0, dated October 1, 2020) which is an integral part of the contract.

v.

f

387. Under this contract, INE authorized Cloudflare, Inc. to process personal data outside the European Economic Area, to any of the 200 servers used by it, as well as the transfer of personal data to the USA.

388. The Defendant had at his disposal the "Cloudflare Data Localization Suite", which contractually allowed him to geographically circumscribe the servers to be used.

389. Successive subcontracting through entities established in third countries was also authorised.

390. Under the terms of the contract, the forum for settling disputes between INE and Cloudflare, Inc. is the California Court.

iv. Violation of the transfer regime

391. The Defendant contracted the services of "Content Delivery Network" (CDN) with the entity Cloudflare, Inc., which was obliged to comply with legislation that removes the protection conferred by the RGPD.

392. These services do not meet the requirements required by law regarding the transfer of personal data to third countries.

393. On April 27, 2021, the CNPD, through Deliberation/2021 /533, ordered the suspension, within a maximum period of 12 hours, of sending personal data from the 2021 Census operation to the USA and to other third countries without a level of adequate personal data protection.

394. On April 28, 2021, the Defendant informed the CNPD of the termination, the day before, of the contract entered into with Cloudflare, Inc.

395. Cloudflare, Inc.'s "Business" package provides its own network of servers, many of which are located in countries that do not ensure adequate protection of personal data.

396. INE authorized Cloudflare, Inc., to process personal data outside the European Economic Zone, to any of the 200 servers used by it, as well as the transfer of personal data to the USA.

397. The decision on which server is used by the citizen who accessed the census form is made by an algorithm, bearing in mind two criteria: the closest proximity of the servers to the place where the form was accessed and the existing availability at any time.

398. From the moment the data entered Cloudflare, Inc.'s network, it was not possible for the Defendant to know and control where the personal data of the respondents circulated.

399. The domain "censos2021 .ine.pt" was resolved to the IP 172.67.41.182, assigned to Cloudflare, Inc., headquartered in San Francisco, USA.

400. US law does not enshrine a level of protection for personal data at least equivalent to that guaranteed by the GDPR.

v. Violation of carrying out an impact assessment on personal data

401. INE did not carry out a DPIA prior to the start of data processing.

402. The AIPD document sent by the Defendant had a circumscribed and insufficient scope, as it did not cover the entirety of the processing, nor even relevant dimensions of the processing of personal data.

403. That document only referred to four personal data processing operations: Processing 1 (IT) Data necessary for contact with the household representative; Treatment 2 (T2) Respondent's data (statistical data provided by respondents when completing the Census form, regardless of the means of transmission of information); Treatment 3 (T3) Data from subcontractors involved in Census activities; Treatment 4 (T4) Resident Population Base.

IV. Decision motivation

404. The facts given as proven resulted from the participation of the inspection activity of the CNPD, and from the Defense contained in the file.

405. After analyzing the evidence produced in the file, jointly and critically, a conviction was formed, based on the facts that were proven.

406. Thus, it is understood that the Defendant's action constitutes the practice of 5 administrative offenses provided for and punished by the RGPD.

407. As a consequence of this, and in view of the verified factuality, the practice by the Defendant, in material authorship, in the consummated form and with possible deceit of the following administrative offences, is sufficiently indicted:

i. An offense provided for and punished by the combined provisions of Article 9(1) and Article 83(5)(a), both of the RGPD, with a fine of up to €20,000,000, for violation of the prohibition processing special categories of personal data;

Av. D. Carlos 1,134,1o

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

ii. An offense provided for and punished by the combined provisions of Articles 12 and 13 and Article 83(5)(b), both of the RGPD, with a fine of up to €20,000,000, for breach of the duties of information to data subjects;

iii. An offense provided for and punished by the combined provisions of paragraphs 1, 6 and 7 of article 28 and paragraph a) of paragraph 4 of article 83, both of the RGPD, with a fine of up to €10,000,000 , for violating compliance with the rules applicable to contracting subcontracting entities;

iv. An offense provided for and punished by the combined provisions of article 44, paragraph 2 of article 46 and paragraph c) of paragraph 5 of article 83, both of the RGPD, with a fine of up to 20,000,000 €, for violation of the transfer regime;

v. An administrative offense provided for and punished by the combined provisions of paragraphs 1 and 2 and paragraph b) of paragraph 3, all of article 35 and paragraph a) of paragraph 4 of article 83, all of the GDPR, with a fine of up to €20,000,000, for breach of the obligation to carry out an impact assessment on the protection of personal data.

V. Determination of the amount of the fine

408. Pursuant to Article 83(1)(a) to k) of the RGPD, the determination of the amount of the fine is based on the following criteria:

The nature, gravity and duration of the infringement taking into account the nature, scope and purpose of the data processing in question, as well as the number of data subjects affected and the level of damage suffered by them - It is considered that the violations committed by the defendant assume a significant degree of seriousness, given the number of data subjects in question (the entire population in Portugal in terms of general data processing, and more than 6 million people in terms of international data transfers) , the context in which they were carried out, in particular, the mandatory response to the 2021 Census and the conviction that questions 29.3 to 29.6 and 30 were mandatory, generated by the conduct of INE. It is also

considered the fact that only two of the administrative offenses for which the Defendant is accused are not punishable by the more serious framework provided for in the RGPD

National Commission

Data Protection

AVG/2021/401

(in this case, violation of compliance with the rules applicable to the contracting of subcontracting entities and the failure to carry out a prior and thorough impact assessment on the protection of personal data);.

Intentional or negligent nature of the infractions and degree of fault:

The. In the case of items i. and ii. of point 407, as a result of negligent action, for not allowing the free formation of the will in the answers to questions 29.3 to 29.6 and 30, and for having violated the duty of transparency embodied in the lack of information to data subjects about the census operation , acting in violation of the duty of care to which, according to the circumstances, he was obliged and capable of doing, acting with awareness of the unlawfulness of the fact;

B. In the case of the offenses indicated in paragraphs iii., iv. and v. of point 407, the Defendant acted intentionally, insofar as he did not comply with the required "due dllHgence" in choosing the subcontractor and signed contract, did not ensure that personal data were only transferred to third countries with adequate protection, nor adopted measures to ensure that the data would always be treated with an adequate level of protection in a third country, in addition to not having carried out the full DPIA prior to the start of data processing; INE was aware of, and could not fail to be aware of, the binding nature of its obligations and accepted the possibility of carrying out the facts of which it is accused, for which reason they are imputed to the Defendant as possible fraud;

iii. The initiative taken by the person responsible for the treatment or by the subcontractor to mitigate the damage suffered by the data subjects - Before being formally notified by the CNPD of the decision ordering the suspension of the transfer of personal data, the Defendant, knowing the meaning of the Decision, suspended the contract with Cloudflare, Inc;

iv. The degree of responsibility of the controller or processor taking into account the technical or organizational measures implemented by him under the terms of articles 25 and 32 - the defendant's responsibility is considered to be high for not having

1200-651 Lisbon

T (+351) 213 928400

F (+351) 213 976832

geral@cnpd.pt

www.cnpd.pt

v-Y'

definition of technical and organizational measures that are minimally sufficient and suitable for the protection of personal information processed;

v. Any relevant infringements previously committed by the controller or processor - which do not occur;

saw. The degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate its possible negative effects - which cannot be considered adequate, insofar as it was necessary to insist on the delivery of the requested elements during the inspection;

vii. The specific categories of personal data affected by the infringement - all personal data collected through the 2021 Census forms relating to the private life of the holders, including data qualified as special (article 9(1) of the RGPD) and data of a highly personal nature25;

viii. The way in which the supervisory authority became aware of the infringement, in particular whether the controller or processor notified it, and if so, to what extent they did so which, in this case, resulted from complaints submitted by citizens;

ix. Compliance with the measures provided for in article 58, paragraph 2, of the RGPD - Following the inspection, and before formal knowledge of the CNPD's decision, the defendant suspended the sending of personal data from the 2021 Censuses to the United States and to other countries without an adequate level of protection and has stopped outsourcing to Cloudflare, Inc., which was required to comply with legislation that removes the protection afforded by the GDPR. Compliance with codes of conduct approved under the terms of article 40 or with the certification procedure approved under the terms of article 42 - a criterion that also does not apply, as there is no code of conduct or certification procedure, under the terms indicated; It is

x. Any other aggravating or mitigating factor applicable to the circumstances of the case, in the light of point k) of paragraph 2

of article 83 of the RGPD, such as the financial benefits obtained or losses avoided, directly or indirectly, through the infringement - With the practice of administrative offenses that are imputed to him, the value of the advantage is unknown

25 Vd. Data Protection Impact Assessment (DPIA) Guidelines. Available at https://ec.europa.eu/newsroom/just/document.cfm?docJd=47711.

obtained by the Defendant through the infractions, but it was found that in the year 2021, the total budgeted income of INE was €68,830,999 (sixty-eight million, eight hundred and thirty thousand, nine hundred and ninety-nine euros); it was also considered, as an aggravating factor, the behavior of the Defendant, during the preparation of the census operation, which revealed a lack of value for the principles and obligations foreseen in the RGPD, when relying on an intervention by the supervisory authority, instead of taking the initiative to ensure that the census operation complied with that regime and to create procedures for this purpose, as well as for the purpose of proving it.

409. In the specific case, we are in the presence of the practice of five administrative offenses, in material authorship and in the consummated form, two administrative offenses practiced with negligence and three with intent, in effective competition.

410. In view of the aforementioned criteria, the CNPD considers it necessary to apply, in this specific case, five fines to the Defendant, considering that this is the effective, proportionate and dissuasive measure that is imposed given the specific circumstances in which the infractions occurred.

411. The framework of fines abstractly applicable to the Defendant is as follows:

i. The combined provisions of Article 9(1) and Article 83(5)(a), both of the RGPD;

ii. The combined provisions of Articles 12 and 13 and Article 83(5)(b), both of the RGPD;

iii. The combined provisions of Article 44, Article 46(2) and Article 83(5)(c), both of the RGPD;

It has a maximum limit of € 20,000,000.00

412. While the framework of the fine abstractly applicable to the following infractions is as follows:

i. The combined provisions of paragraphs 1, 6 and 7 of article 28 and paragraph a) of paragraph 4 of article 83, both of the

RGPD;

ii. The combined provisions of paragraphs 1 and 2 and paragraph b) of paragraph 3 of article 35 and paragraph c) of paragraph 4 of article 83, both of the RGPD;

It has a maximum limit of €10,000,000.00.

Av. D. Carlos 1,134,1o

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

v.

{

413. Assessing the facts found in the light of the above criteria, the CNPD, under the terms of article 58(2)(b) of the RGPD, considers appropriate the application to the Defendant of:

i. A very serious fine, for lack of lawful basis for the collection of special data, the infringement of which was committed with negligence, in the amount of €1,600,000 (one million, six hundred thousand euros);

ii. A very serious fine, for violation of the duty to inform the holders of personal data, whose infringement was committed with negligence, in the amount of €1,600,000 (one million, six hundred thousand euros);

iii. A fine for violating the rules applicable to the contracting of subcontracting entities, whose infraction was practiced with malice in the amount of €200,000 (two hundred thousand euros).

iv. A very serious fine, for violation of the regime for the transfer of personal data, the violation of which was committed with malice, amounting to €2,400,000 (two million, four hundred thousand euros);

v. A fine for breach of the obligation to carry out an impact assessment on the protection of personal data, whose infringement was committed with intent, in the amount of €400,000 (four hundred thousand euros);

414. Added to the 5 partial fines, it results in a value of €6,500,000 (six million, five hundred thousand euros).

415. After framing the partial sanctions, it appears, in accordance with paragraph 3 of article 83 of the RGPD, that "[whether the person responsible for the treatment or the processor violates, intentionally or through negligence, within the scope of the same processing operations or operations linked together, various provisions of this Regulation, the total amount of the fine may not exceed the amount specified for the most serious breach".

416. In the present case, the amount specified for the most serious violation is €20,000,000 (twenty million euros), which constitutes the abstractly applicable maximum limit.

417. It also provides for paragraph 3 of article 19 of the RGCO, applicable alternatively, ex vi article 45 of Law no. 58/2019, of August 8, that «The fine to be applied cannot be lower than the highest of the fines specifically applied to the various offences», that is to say €2,400,000 (two million, four hundred thousand euros).

418. We have, then, that the abstract frame of the single fine to be applied is between a minimum of €2,400,000 (two million, four hundred thousand euros) and a maximum of €20,000,000 (twenty million euros).

SAW. Grounds for applying the single fine

419. The essential prerequisite for the effectuation of the legal accumulation of partial fines is the commission of several infractions by the same Defendant before the final conviction for any of them becomes final.

420. In this sense, in order to carry out the legal combination, it is necessary to verify the following requirements, of a procedural and material nature, (i) that they are sanctions related to administrative offenses committed before the final and unappealable conviction for any of them, (ii) that have been committed by the same Defendant and that the sanctions are of the same nature.

421. 0 which is verified cumulatively in the present case, thanks to the existence of the effective or pure competition, either in the real competition aspect, or in the ideal competition aspect.

422. Given the conduct expressed by the vast and serious set of offenses committed, by the vast and extended number of

potential holders of personal data affected and very specifically by the lack of freedom of citizens in providing their special or sensitive data - insofar as the response to the censuses is mandatory and the provision of such data appeared to be so - it is understood that a sanction is due that translates the high censorship of this behavior, which will translate into a concrete fine whose value will serve as a dissuasive effect of identical behaviors in the next operation census.

423. When considering the single fine to be applied, and without prejudice to the high degree of censure of the Defendant's conduct, reflected in the indifference of the new applicable legal framework, the CNPD considers relevant the fact that the Defendant has no history of applying administrative offenses for violating data protection regulations.

424.Now, considering the legal assets protected by the administrative offenses in question, which he committed, it seems effective, proportional and dissuasive, the application to the Defendant:

i. As a legal sum, pursuant to the combined provisions of Article 83(3) of the RGPD and Article 19(3) of the General Regime of Offenses, a single fine of €4,300,000.00 (four million and three hundred thousand euros).

Av. D. Carlos 1,134,1o

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

v.

, f

VII. Conclusion

425. In view of the above, the CNPD decides:

i. Do not sanction the Defendant for the practice of the following offenses:

The. An offense provided for and punishable by the combined provisions of Article 5(2) and Article 83(5)(a), both of the RGPD, with a fine of up to

20,000. € 000, for violation of the liability principle;

B. An offense provided for and punishable by the combined provisions of paragraph a) of paragraph 1 of article 5 and paragraph a) of paragraph 5 of article 83, both of the RGPD, with a fine of up to €20,000,000, per violation of the principle of legality, loyalty and transparency;

w. An offense provided for and punished by the combined provisions of Article 37(7) and Article 83(4)(a), both of the RGPD, with a fine of up to

10,000. 000 €, for breach of the duty to communicate, to the Control Authority, the designation of the Data Protection Officer;

d. An offense provided for and punishable by the combined provisions of paragraph c) of paragraph 1 of article 5 and paragraph a) of paragraph 5 of article 83, both of the RGPD, with a fine of up to €20,000,000, per violation of the principle of data minimization;

It is. An administrative offense provided for and punished by the combined provisions of article 37 and subparagraph a) of paragraph 4 of article 83, both of the RGPD, with a fine of up to

10,000. €000 for breach of duty;

ii. Apply to the Defendant National Institute of Statistics:

The. A single fine, in the amount of €4,300,000 (four million, three hundred thousand euros);

426. Pursuant to paragraphs 2 and 3 of Article 58 of the General Regime of Offenses, inform the Defendant that the conviction becomes final and enforceable if it is not judicially challenged under the terms of Article 59 of the same statute. , within 20 working days of notification.

427. The Defendant must pay the fine, within a maximum period of 10 days, after its final nature, sending the respective payment slip to the CNPD. In case of impossibility of timely payment, the Defendant must communicate this fact, in writing, to the CNPD.

Approved at the meeting of November 2, 2022

Ana Paula Lourenço (Rapporteur)

Conceição Diniz

Tilipa Calvão (President)

Av.D. Charles 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400 geral@cnpd.pt

F (+351) 213 976 832 www.cnpd.pt

w

National Commission

Data Protection

Process AVG/2021/401

Cone: On 2.11.2022

Pursuant to subparagraph h) of paragraph 1 of article 19 of Law no. 43/2004, of August 18, and on the basis of Deliberation/2022/1072 of this Commission, of November 2, I hereby ratify the said Deliberation and, consequently, I apply, to the defendant, Instituto Nacional de Estatística, I.P. for committing five administrative offences, in legal combination, under the terms of the combined provisions of article 83(3) of the RGPD and article 19(3) of the General Regime of Offenses, the single fine of 4,300. €000.00 (four million three hundred thousand euros). .

Notify

d.s.

The president,

(Filipa Calvao)

Av. D. Carlos 1,134,10

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt