rJ

CNPD

Nachronal Commission

of Data Protection

l. Introduction

AVG 12021 I 401

1

DELTBERATION/2021t533

i. The National Data Protection Commission (CNPD) received more than a dozen participations concerning to the ongoing census operation - 2021 Census - carried out by the National Statistics Institute, l.P. (INE), the which in part takes the form of filling in the form available online at the address httos.//censo s2021.ine.pt/ The largest participation is related to the fact that the survey obliges to provide citizens' identification data, namely their full name. However, some shares associated the obligation to provide identified data with the transfer of data to a company based in the United States of America.

2. The same question was also asked on social networks, with media outlets reporting that the information presented there was not accurate.

3. The CNPD, under the powers conferred by subparagraphs b) and eJ of paragraph 1 of article 58.0 of Regulation (EU) 20161679 of the European Parliament and of the Council of 27 April 2016 (General Regulation on the Protection of Data - RGPD), in conjunction with the provisions of article 3.0, paragraph 2 of article 4.0 and paragraph b) of paragraph 1 of article 6.0, all of Law n.0 58/2019, of August 1st (which aims to ensure the execution, in the order internal legal system, of the RGPD), analyzed the INE website and the platform available there, having concluded that this entity uses services provided by the company Cloudflare. It was still requested information to iNE regarding this operation on personal data.

ll. Analysis

i. established facts

4. The 2021 Census data collection form is accessed through the available infrastructure

by Cloudflare, lnc. (hereinafter, Cloudflare), a company based in San Francisco, California, in the United States

United States of America. This company provides various Internet security and Content Delivery services

Network (CDN).

5. The CDN consists of a network of servers that aims to reduce the latency of access to the

servers - 1.e., the period of time that elapses between the user's action and the response to that action. With

In effect, through an algorithm that simultaneously enters the information for several servers, chooses the one

which has a shorter response time. with islo, the fastest information delivery is achieved

and more robust from a security point of view.

Av. D. Caíos l, 134, 1o

'1200-651 Lisbon

l (+351) 213 928 400

F (+351)213 976 832

gerâl@cnpd.pt

www.cnpd.pt

AVGt2021t401

1v

6. Cloudflare has two hundred (200) datacenters located in more than one hundred countries, the vast majority of

which do not have an adequate level of data protection, pursuant to Article 4 of the GDPR.

7. INE used services provided by the company Cloudflare through the online subscription of its Busmess

p/an'. This plan provides a set of services, with INE currently making use of WAF2,

CDN, and Rate lrnrit3.

B. Said plan is governed by the 'self-serve subscription Agreement'a (main contract for the provision of

services) and the data processing addendum (Data Processing Addendum version 3.0s), dated

1 October 2020, which is a part of the main contract (see clause 6.1 of the main contract).

9.0 INE justified the execution of this contract in order to '(..) respond effectively to the

performance and information security needs associated with the size and complexity of the operation

2021 Census".

I0. Notwithstanding the use of this service, it is not and has never been in question that the information provided by citizens through the 2021 census forms is hosted on the INE servers.

11. When citizens access the 2021 Census form, they are forwarded to one of the Cloudflare according to said algorithm. Although the criterion underlying this algorithm is that of the greatest proximity of the servers in relation to the place of origin of the invocation, there is no guarantee that this will happen, since it depends on the load existing on them at any given time. Cloudflare infrastructure communicates with the INE server via TLS.

1 2 The name censos2021 .ine.pt is associated with IP 172.67 .41 .182, located in the United States of America, being assigned to CloudÍlare. Customers access the site using the secure communication protocol HTTPS, the associated certificate being issued by Cloudflare, tnc ECC CA-3, a certification body from Cloudflare itself. In this way, this company owns both the private key and the public key,

r This plan is featured on the Cloudflare website as intended for small business and e-commerce websites, which advanced performance and security, giving priority to the support of .orr... ãta,óni.o. saw https://www.cloudÍlare.com/plans/business/

2 A WAF helps protect web applications by filtering and monitoring HTTP traffic. Pyotege of attacks like cross slre Reguest Forgery,

Cross S,te Sci,pÍlng, SoL /r.iectior, among others.

3 Ráte ,r?itlng protects against Oenial of service (DoS) attacks, brute force attacks and other types of malicious behavior.

I https://www cloudflare.com/terms/

thus being empowered to cilrage and decrypt all communications between citizens who access

to the form and send data to the lNE server.

13. Note that the fact that the encryption key used is from Cloudflare means that the encryption is applied by

this entity, maintaining itself during the transit of information, and it is by it, and only by it, deciphered - that is,

before the delivery of the set of information (the data packets) to the lNE, Cloudflare must proceed with its

decryption, with INE not having any intervention in this process.

14. Furthermore, Statistics Portugal admits that it has no control over the transmission of information between citizens and

their service.

Once inside Cloudflare's CDN network, INE has no way of knowing if traffic is being directed to

servers located in the territory of European Union countries, or resident in any other part of the globe.

15. Up to the date of this deliberation, personal data of more than six million citizens have been collected

residents in national territory.

ii. Appreciation in light of the GDPR

16. There being no doubt that the information provided by citizens when filling in the forms

Censuses 2021 constitute personal data, pursuant to article 4.0, paragraph 1), of the GDPR - as they correspond

to information relating to identified natural persons - the census operation is subject to the RGPD, being

the INE is responsible for the treatment, in accordance with paragraphs 2) and 7) of the same article.

17. While still certain that some of the information falls into the category of special personal data provided for

in paragraph 1 of article 9.0 of the GDPR, and therefore the processing of data is subject to a stricter protection rule.

rigorous and, therefore, the obligation to carry out an impact assessment on data protection

(AIPD), in accordance with Article 9.0, paragraph 1 and subparagraph b., of Article 9.0 of the GDPR.

18. It is noted that the IAPD has to cover all operations on personal data, including, therefore,

the operation corresponding to the transport of information to and from Cloudflare's servers, within the scope of

subcontracting relationship.

19. On this point, Statistics Portugal told the CNPD that '(...) it chose to carry out an Impact Assessment

over Data Protection only to the main statistical operation. This was due to the fact that the tests

(2016,2018,2020) are only intended to test collection processes and application functionalities, and to be, as far as

it concerns the applicational, partial solutions. Therefore, they did not allow testing and evaluating the risk inherent to sludge.

the processes. In this sense, only the final operation allowed a complete and comprehensive evaluation to be carried out.

Av. 0. Carlos I, 13410

120M51 Lisbon

I (+351)213 928 400

F (1351) 213 976 832

geral@cnpd. en

www.cnpd.pt

in a scenario in which the current decisions, given the pandemic context, were being changed and optimized. At the

however, the respective contents are not yet integrated in order to be available in a

immediate. Although the systematic and continuous monitoring of the EpD and the RS/the Census is guaranteed

2021 .',

20. As an impact assessment was not carried out for this specific operation on the data

data, Statistics Portugal did not carry out a risk assessment for the rights of data subjects and,

consequently, it did not adopt any supplementary measure to mitigate these

risks, having only focused on the performance and security of the system, including promoting a

consultation with the National Security Office.

21. On this operation, INE did not consult the CNPD, which would have allowed the CNpD to comment and thus seek to safeguard the rights of data subjects.

22. However, even considering the purpose pursued with this operation, there were other solutions that would allow the mitigation of risks, guaranteeing INE greater control over the data, and, from the outset, limiting the transit of personal data to the territory of the Member States of the European Union, not implying its sending country third States.

23.0ra, the INE's option implies, as will be shown, the transit of personal data through third countries in in relation to the European Union and that do not have the adequate level of protection. It also implies, by virtue of the signed contract, a specific authorization from the INE for the transfer of personal data to the States United States of America (USA) and other countries where the servers used by cloudflare (namely, south africa, china, india, jordan, mexico, russia, singapore)

24. As described above, in points 5 and 1 1, the personal data of citizens residing in Portugal are sent to Cloudflare servers located in different countries neither identified nor identifiable by the INE or by the data subjects. In addition, the encryption and decryption key is owned by Cloudflare.

25 0r4, the contract entered into by INE and Cloudflare provides for the transit of personal data to anyone of the 200 servers used by it, as well as the transfer of personal data to the USA.

26. Indeed, pursuant to the Daía Processing Addendum version 3.0 (hereinafter, DpA), which, it is recalled, includes 0 contract, personal data of the customer (data exporter) is transferred to Cloudflare (importer of data), in the United States of America, using as an international transfer mechanism the standard contractual clauses based on Commission Decision 2010/87lUE of 5 February 2010, applicable

to transfers of personal data to subcontractors established in third countries6, which

an integral part of the addendum and are, to that extent, subscribed by the customer (cf. point m) of clause 1.1 of the DPA)7.

27. The DPA applies to the extent that Cloudflare shares personal data submitted by the customer to CloudÍlare

or, as is the case with the INE, collected and processed by the customer who uses the service, when such personal data

are subject to applicable data protection legislation.

28. Thus, by (sub)contracting Cloudflare's services, the INE, in its capacity as controller

and simultaneously as a customer, accepted the conditions of use of the service, including the addendum to the terms of

processing of personal data, which contains a conIict between the controller (INE) and the

subcontractor (Cloudflare) for the transfer of personal data to the United States of America.

29. Also in accordance with the terms of the DPA, the INE granted Cloudflare a general authorization for it to

may resort to others (sub-contractors, whether companies within or outside the Group (clause 4.2),

recognizing and accepting that recourse to (sub-

)subcontractors established in third countries (clause 6.4).

30, Whether standard contractual clauses are, in general, a legal instrument for the transfer of data

personal data to third countries, under the combined provisions of Article 46.0, paragraph 2, c) and paragraph 5, of the

GDPR, it is necessary to verify, however, whether the legislation of the third State, which obviously overlaps with a

instrument of a contractual nature, does not diminish or empty the guarantees offered by these clauses, the

which precisely aim to compensate for the lack of an adequate level of protection in the country of destination

data (cf. article 44.0 and 46.0 of the GDPR)8.

31. According to the Court of Justice of the European Union (CJEU), it is up to the data exporter,

on a case-by-case basis, with the collaboration of the data importer, verify that 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

keep me. This obligation also stems from compliance with the principle of responsibility, enshrined in

in article 5.0, paragraph 2, of the GDPR.

ô As per Cloudflare's website, privacy policy was revised on October 27, 2020, country

legal instrument on which the transfer of personal data from the European Union (EU) to the United States of America (USA) is based, which

is no longer the adequacy decision of the Privacy Policy (Privacy Sh/e/d.), invalidated by the Federal Court of Justice European Union (CJEU), in July 2020, in the case of Schíems //, in order to change the contractual clauses

7 https://w',^/w.cioudfiare.com/cloudflare

8 Vel n 0s 92 and 93 of Judgment Schrems /i, in which the Court pointed out 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 irrespective of the use of a mechanism of

Transference mentioned in Chapter V of the RGP0.

q See paragraph 134 of the Schrems judgment //.

cuslomer SCCs odí

Av. D. CâÍlos I, 1 34 1

120M51 Lisbon

The

T (+3s1) 213 928 400

F (+35i) 213 976 832

geral@cnpd.pt

,â/ww.cnpd.pt

AVG/2021/401

3v

I

32. According to the CJEU's analysis in the Schrems // case, US legislation - which is the country of destination for Cloudflare's international transfers under standard contractual clauses - enables interference

fundamental rights of people, based on requirements relating to national security and the

public, which may result in access to personal data transferred from the EU to the US and the use of those

data within the scope of surveillance programs, based on Section 702 of the FtSA (Foreign Intelligence Surveillance Act) and Executive Decree 1233310.

33. The CJEU concluded that such interferences are not proportionate, in the light of Union law, insofar as they the scope of limitations on people's rights is not defined, there are no clear and precise rules regarding the application of these measures or minimum requirements for protection against risks of abuse, there is no 1cause of necessity, and no enforceable rights are granted to the data subjects or remedies jurisdiction, so the limitations on data protection arising from US law do not satisfy The requirements required by the uElr Charter of Fundamental Rights (cf. articles 7.0, g.0, 47.0 and 52.0, no. 1).

34. Therefore, it would only be possible to carry out a transfer of personal data to the USA if the legislation concerned herein, and expressly referred to by the CJEU, were not directly or indirectly applicable to Cloudflare or yours (sub-subcontractors, and even then only through the adoption of supplementary measures that could demonstrably prove that this legislation would not be applicable or would not have practical effect in the transfers of personal data.

35. However, the services provided by Cloudflare, namely those contracted by INE when subscribed to the Euslness P/an, place the company directly under the US legislation that imposes it the obligation to grant bulk access to personal data processed by you, as a provider of electronic communications services, without prejudice to other types of services being also covered by other provisions of US surveillance legislation.

36. Cloudflare recognizes in point 7 of the DpA that, in its role as a subcontractor, 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 client, ie the GDPR. In this case, if there is a conflict of laws, Cloudflare declares that it will immediately inform the customer, «unless such notification is strictly prohibited» (cf. subparagraph a) clause 7.1).

r0 VeÍ n.0 165 of the cited document, in which the pRlSi.4 and UpSTREAtú programs are cited

See Nos. 75-176, 180, 185, 191 and 194 of the judgment cited.

r2 Cf. Section 702 of the FISA as amended by 50 USC s lBBt â.

37. This is precisely the case with this US legislation which prevents US companies from inform their customers of the access made by the US authorities to collection points for information on foreigners in the context of national security activity.

38. It appears, therefore, that there is no guarantee that the personal data of citizens residing in Portugal, collected by INE through its website, within the scope of Census 202.l, are not accessed by the authorities of the USA, by means of Cloudflare due to the services provided by it to INE and which imply, as signed contract, the transfer of such personal data to the USA.

39. In this sense, as standard contractual clauses, under which personal data are transferred by INE to Cloudflare, in the USA, are respected in the third country of destination, insofar as these do not bind the authorities of that country, thus not offering the adequate guarantees required by the GDPR, the CNPD is obliged to prohibit these data transfers, in accordance with the provisions of the ÍJUE.r3

40. In addition, according to the same jurisprudence, even if the INE could demonstrate that the data personal data were not transferred to the US, the transit of the data would always depend on the adoption of measures adequate and suflcient supplementary measures, which are not present here.

41. Under the terms of paragraph 2 of article 5.0 and article 24.0 of the RGPD, the INE is obliged to comply with the principles and rules for the protection of personal data, as well as demonstrating the compliance of the treatments of personal data under your responsibility.

lll. Conclusion

42. In view of the foregoing and as there is no other corrective measure capable of safeguarding the rights of the titleholders of the data, the CNPD resolves, under paragraph 2 of article 58.0 of the RGPD, to order the National Institute

of Statistics, 1.P., the suspension of sending personal data from the 2021 Census to the US and other countries third parties without an adequate level of protection, either through Cloudflare, Inc., or another company, within the maximum of 12 hours.

43. The same entity must also ensure, within the scope of possible subcontracting, that the subcontractors are not obliged to comply with legislation that departs from the protection provided by the GDPR.

r3See n.0 107 and 121 of the cited decision.

ra cf. paragraphs 63 and '183 of the same judgment

Av. D. Carlos 1,134,10

1200{51 Lisbon

T (+351)213 928 400

F (+35',1) 213 976 832

geral@cnpd.pt

r/vww.cnpd.pt

44. The hearing is waived, under the terms of subparagraph a.) of paragraph 1 of article 124.0 of the Code of Procedure Administrative, considering the urgency of the corrective measure, taking into account the time period of the Ícholha Census online and that, otherwise, lisco would be maintained for the rights, freedoms and guarantees of the citizens, potentially more than four million, who have not yet complied with the legal obligation to respond to the census operation.

Approved at the meeting of April 27, 2021

Filipa Calvão (President)