

/ NATIONAL COMMISSION ON DATA PROTECTION

OPINION/2020/108

I. Order

Instituto de Informática, IP, (II) has asked the National Data Protection Commission (CNPd) to comment on a model agreement for the regulation of operations and processing of personal data in which it will intervene as a subcontractor.

The CNPD pronounces itself, as the national authority for controlling the processing of personal data, within the scope of subparagraph b) of paragraph 3 of article 58 of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 of April 2016 (General Regulation on Data Protection - RGPD), in conjunction with the provisions of article 3 and paragraph 2 of article 6, of Law no. August.

II. appreciation

The document sent, known as the Framework Agreement (hereinafter the agreement), is intended to be the act that will regulate the relations between the controllers and the II in the various subcontracting operations, in compliance with Article 28(3) of the GDPR.

Bearing this context in mind, it is suggested to change the title so that it reflects the scope of the agreement, therefore referring to data protection legislation and not only to the GDPR. The same goes for points B. and C. of the recitals.

Also with regard to point B. of the recitals, where it is stated that compliance with the rules underlying the collection and processing of Personal Data is required; Data security and privacy, it is suggested to eliminate the term collection, since it is contained in the concept of data processing as defined in paragraph 2) of article 4 of the RGPD; it is also suggested the densification of the term security and, finally, the elimination of the term data privacy, as it corresponds to a concept used in Anglo-Saxon law that has no correspondence in the European and national data protection legal regime.

Therefore, as it is more in line with the requirements of personal data protection legislation, it is recommended that recital B. be replaced by the following wording: Compliance with Data Protection legislation requires the establishment of rules underlying the processing of data personnel and the adoption of technical and organizational measures

Av. D. CARLOS I, 134 - 1o | 1200-651 LISBON | www.CNPd.PT | TEL: +351 213 928 400 | FAX: +351 213 976 832

Process PAR/2019/67 1v.

adequate to guarantee a level of security appropriate to the risk to the rights and freedoms of the holders.

Looking now at the clauses of the agreement, it is recommended, for the reason already explained, the elimination of the term collection in Clause One.

No. 2 of Clause Three, by the examples contained therein, seems to admit several purposes. However, this reality implies that Annex I of Clause Two is organized in such a way as to separate the set of personal data by processing purpose. Therefore, it should be considered that the clause listing the purposes of the treatment is prior to the clause indicating the categories of holders and the personal data processed for each purpose.

With regard to paragraph 3 of Clause Three, the CNPD is unable to reach its meaning.

With regard to Clause Four, the obligations of the person in charge and the subcontractor are established. However, two issues are immediately identified that are not regulated, namely: the subcontractor's obligation to inform the person responsible for successive subcontracts and the need to obtain a declaration of non-opposition¹ (cf. Article 28(2) of the GDPR) and the conditions for complying with the subcontractor's obligation to inform the person responsible in the event of a personal data breach (cf. Article 33(2) of the GDPR). It is therefore recommended to regulate these two aspects in the aforementioned Clause.

Regarding the obligation to guarantee the exercise of the rights of the data subjects that, in subparagraph a) of paragraph 2 of Clause Five, falls on the processor, it is noted that this is a typical obligation of the controller, under the terms of Article 12(1) of the GDPR. Consequently, it is recommended that it be removed from the subcontractor's set of obligations.

As for the security measures contained in Clause Seven, the GDPR requires that, in addition to confidentiality and integrity, the permanent availability and resilience of the systems be ensured.

In paragraph 2 of this clause there seems to be a clear wording error, as technical and organizational measures are required to prevent "accidental or legal access". Presumably intended to assert accidental or intentional access.

¹ Clause Six appears to be the general authorization provided for in Article 28(2) of the GDPR.

Process PAR/2019/67 2

• JfSfr

JT NATIONAL COMMISSION

' DATA PROTECTION

As the CNPD does not know the Security and Privacy Policy of //, it cannot comment on paragraph 4 of this clause.

Finally, the advisability of including in the agreement, as an obligation of the processor, the registration of all categories of processing activities carried out on behalf of a controller, in accordance with the provisions of Article 30(2) is underlined. ° of the GDPR, as well as the obligation to assist the controller, if necessary and at his request, to ensure compliance with the obligations arising from carrying out impact assessments on data protection and from prior consultation with the supervisory authority, in in line with recital 95 of the GDPR.

III. Conclusion

The CNPD understands that, with the changes arising from the above considerations, the Framework Agreement may be the model agreement for the regulation of operations and processing of personal data in which Instituto de Informática, IP, will intervene as a subcontractor. It should be noted, however, as explained above, that there are matters on which the CNPD has not commented as it does not have the elements to do so (No. 3 of Clause Three and No. 4 of Clause Seven).

Approved at the meeting of September 8, 2020

Filipa Calvão (President)

AV. D. CARLOS 1, 134 - lo I 1200-651 LISBON I WWW.CNPD.pt I TEL:+351 213 928 400 | FAX: +351 213 976 832