/ NATIONAL COMMISSION t. DATA PROTECTION

i

OPINION/2020/85

I. Order

The Social Security Institute, I.P. (ISS) submitted a draft protocol for consultation to the National Data Protection Commission (CNPD) on electronic communications between judicial courts and Social Security, within the scope of technical advice provided to the courts in the context of civil and civil tutelary proceedings. promotion and protection.

The CNPD issues an opinion within the scope of its attributions and competences as an independent administrative authority with powers of authority to control the processing of personal data, conferred by subparagraph çj of paragraph 1 of article 57 and by paragraph 4 of article 36 . of Regulation (EU) 2016/679, of 27 April 2016 - General Data Protection Regulation (GDPR), in conjunction with the provisions of article 3, paragraph 2 of article 4. and in paragraph a) of paragraph 1 of article 6, all of Law n.° 58/2019, of 8 August.

The draft protocol under consideration (hereinafter the “Protocol”) identifies the Instituto de Gestão Financeira e Equipamentos da Justiça, I.P (IGFEJ)1, the Instituto de Informática, I.P. (II), the Social Security Institute, I.P. (ISS), the Social Security Institute of Madeira, IP-RAM (ISSM) and the Social Security Institute of the Azores, IPRA (ISSA).

The Protocol defines the terms of collaboration between the parties, with a view to electronic communications within the scope of technical advice to the courts (ATT) in judicial proceedings for the promotion and protection and civil guardianship of children and young people in danger who reside or are in national territory. (cf. Clause One).

In this way, the courts, through the IGFEJ, send requests or requests for information within the scope of judicial proceedings to the ISS, the ISSM and the ISSA, through the II, receiving the respective responses to their requests, as well as interim information from the services. of social security.

The protocol precisely lists the categories of data transmitted, which include, among others, the data identifying the case (identification of the court and the ATT team, court case number, area of activity (promotion and protection, civil tutelage or

1 Which intervenes as a subcontractor of the Courts of Justice, under the terms of item 8) of article 4 of the RGPD.

administrative), date and number of the act, type of process and request, as well as the personal data of the intervening parties, including name, address, date of birth, civil and tax identification number and type of intervenient. The sending of associated documents is also foreseen (cf. Clause Three).

Communications are carried out between the systems of the granting entities, using web services, with a duly accredited application user, through the dedicated circuit between the IGFEJ and the II, with the information being internally directed to the geographic area of the recipient ATT or, in in the opposite direction, from the competent court, and being available in real time (cf. Clause Four).

Clause Five prescribes that access to information is preceded by authentication between iGFEJe and //, by validating the user's access, as well as maintaining the record that identifies the user is the responsibility of the final entity that calls the service (n. 1).

It is also up to the final entity to guarantee security, adopting the appropriate technical or organizational measures, namely restriction of access to data, definition of different profiles, restriction of access by geographic areas, impossibility of consultations if it does not intervene in the process. (No. 2).

It is also foreseen that the II, under the terms of its audit policy, will proceed to the registration of all consultations carried out within the social security as well as all accesses from abroad.

Clause Six identifies IGFEJ and II as processors and ISS, ISSM and ISSA as controllers, within the scope of this Protocol, providing for the possibility of subcontracting processing activities subject to the written authorization of the responsible for the treatment.

Clauses Seven and Eight provide, respectively, on the obligations of controllers and processors. Clause Ten regulates aspects of the protection of the rights of the holders of personal data. The obligation to adopt information security measures, in compliance with article 32 of the RGPD, as well as the obligation of confidentiality are provided for, respectively, in Clauses Eleven and Twelve. The remaining clauses, up to the fifteenth, provide for the applicable legislation, the parties' interlocutors, the validity and conditions of termination.

llif

II. appreciation

The Protocol in question thus complies with paragraphs 1 and 6 of article 2 of Ordinance no. of civil tutelage and promotion and protection proceedings, are carried out in a structured manner and electronically, through the signing of a protocol between the entities identified above as grantors.

This ordinance thus comes to fruition, in the context of Law no. general regime of civil tutelage proceedings, and considering Decree-Law no. the courts and the technical advice provided to them by Social Security.

Thus, it is considered that the basis of legitimacy for this processing of data is based on subparagraph c) of paragraph 1 of article 6 of the GDPR, and, when there is processing of special categories of data, in the combined provisions of subparagraphs b) and f) of Article 9(2) of the GDPR.

With regard to the conditions of access to information, it is considered that the wording of Clause Five needs clarification, since it does not result from paragraph 1 that the activity of the individual end user is recorded, in addition to the registration of the user. application, which is a generic user.

However, it is essential that the respective social security and court systems record the activity of individual end-users for auditing purposes, allowing their activity to be traced. For this purpose, users will also have to be individually accredited in the respective systems in order to allow individual authentication per user. Likewise, this protocol should provide for the retention period of these audit logs, both in the justice system and in the social security systems, depending on the purpose of the processing.

Paragraphs 3 and 4 of this clause should be made more explicit in order to understand exactly what interactions they refer to. Furthermore, communications between the II and the ISS, the ISSM and the ISSA must be reflected in the protocol.

With regard to paragraph 2, although we agree with the general content of the rule, it is not sufficiently clear who is the final entity, whether the controllers, the subcontractors IGFEJ and II, through which the circuit is established dedicated.

Also in relation to paragraph 5 of this clause, which refers to the archival conservation regulations applicable to personal data processed by Social Security, the reason for its inclusion in this protocol is not understood, since in this area new treatments

are not established. of data in addition to those that the law already provides, only by changing the means of communication of the data. The retention periods for personal data processed within the scope of technical advice to the courts will be those that the law provides for this case, so this number must be eliminated.

With regard to point g) of Clause Eight, which provides that processors comply with the rules defined by the controllers to proceed with the transfer of data to third countries or international organizations, it must be deleted, as there is no legal provision international transfer of personal data that processors may make under this Protocol.

Given the highly sensitive personal data in question and the fact that they arise from legal proceedings, in addition to involving minors, it will certainly not be on the horizon of those responsible for data processing to authorize their subcontractors (IFGEJ and II) to use services under of subcontracting to companies established outside the national territory, also in countries outside the European Economic Area, which would hardly present sufficient guarantees in this context.

Regarding Clause Ten, it is considered that subparagraph a) has a content contradictory to subparagraph b), since the first provides that the data controller is responsible for satisfying requests for the exercise of rights by data subjects. , while the second points to the exercise of rights being carried out with subcontractors. also don't

achieves the objective of subparagraph c) of this clause, in particular with regard to the rights of data subjects, so its elimination is suggested.

In relation to paragraph 2 of Clause Ten, its inclusion in the text of the protocol is not considered appropriate, since the obligations of controllers, namely the guarantee of the rights of the holders, as provided for in subparagraph a), stem from the law. In addition, point b) is reductive as to the information that must be provided to the holders, which is provided for in articles 13 and 14 of the GDPR and cannot be restricted by protocol. Point d) should also be deleted, as the controllers do not have to demonstrate to the subcontractors the lawfulness of the processing they carry out.

In short, it is understood that this clause should be deleted or, at least, entirely revised in the light of the observations made.

With regard to Clause Twelve, it should be noted that paragraph 3 of it, imposing a confidentiality agreement with the workers who participate in the processing operations, is excessive, insofar as it is a matter of a protocol between public entities, whose workers are already legally bound to secrecy, either in the courts or in social security. As for possible workers at the service of

other subcontractors, the confidentiality agreement is already covered in subparagraph d) of Clause Eight.

Finally, the identification of the parties' interlocutors and their respective contacts for the purpose of monitoring the execution of the protocol is considered positive, as well as the obligation to carry out all communications in writing.

III. Conclusion

Based on the above observations, the CNPD considers, in general terms, that:

1. It is essential to clarify the wording of Clause Five, explaining in particular that the activity of individual users is recorded for audit purposes, thus making it possible to track their activity. The period of conservation of these fogs must also be recorded in the protocol, as well as paragraph 5 must be eliminated;

2. Paragraph 5 of Clause Eight must be deleted, as there is no legal provision for international data transfer in the context of personal data processed within the scope of this protocol;

3. The Tenth Clause must be completely revised, if not deleted, and contain only rules that are relevant, if any, for the exercise of the rights of the holders, according to the clause's epigraph.

With the introduction of the changes identified above and duly detailed throughout the opinion, the CNPD considers that there are no impediments to the conclusion of the protocol on electronic communications between the judicial courts and Social Security, within the scope of technical advice to the courts.

Approved at the meeting of July 28, 2020

Filipa Calvão (President)