National Data Protection Commission

OPINION/2022/40

I. Order

1. The Insurance and Pension Funds Supervisory Authority (ASF) requested the National Data Protection Commission (CNPD) to issue an opinion on the draft regulatory standard on market conduct and the handling of complaints by this authority .

2. 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 c) of paragraph 1 of article 57, subparagraph b) of Article 58(3) and Article 36(4), all of Regulation (EU) 2016/679, of 27 April 2016 - General Data Protection Regulation (hereinafter GDPR) , in conjunction with the provisions of article 3, paragraph 2 of article 4 and paragraph a) of paragraph 1 of article 6, all of Law No. 58/2019, of 8 of August, which implements the GDPR in the domestic legal order.

3. However, at the request of the CNPD, an impact assessment on the protection of personal data (AIPD) was presented.

II. Analysis

4. The legal framework for accessing and exercising the insurance and reinsurance activity (R JASR), approved by Law No. 147/2015, of 9 September, and the legal framework for the constitution and operation of pension funds and entities pension fund managers (RJFP), approved by Law No. the insurance activity and the pension fund management activity, which determine the need to review the currently applicable regulations, adapting them to the new legislation governing the aforementioned activities.

5. Pursuant to article 159 of the RJASR and article 149 of the RJFP, it is incumbent upon the ASF to establish, by regulatory rule, the general rules to be respected by insurance companies and pension fund management entities in fulfilling the duties provided for in terms of market conduct, which is now being done.

6. Under the terms of the preamble, this draft regulatory standard also aims to update the regime applicable to the

management of complaints, to the customer's ombudsman and to the interlocutor before the Insurance and Pension Funds Supervisory Authority (ASF), and extends the scope of application of the policy for the treatment of policyholders, policyholders, beneficiaries or third parties injured in the activity of managing insurance funds

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

pensions, regulating the relationship between managing entities and associates, contributors, participants and beneficiaries.

7. The project also aims to adapt and systematize the requirements applicable to reporting for the purpose of behavioral supervision and establishes that insurance companies and management entities must have an autonomous website that includes a specific tab with information dedicated to the matter. of market conduct.

8. Finally, in line with the provisions of articles 157 of the RJASR, 198 of the RJFP and 76 of the legal regime for the distribution of insurance and reinsurance, approved by Law No. 7/2019, of 16 January, the procedures applicable to the handling of complaints presented to the ASF regarding acts or omissions of the supervised entities are implemented.

9. Thus, the project includes the processing of personal data of the customer's provider or the provider of participants and beneficiaries and of the members of the respective management or administration body (identification data and contact data and curriculum vitae), full name and contact details of the claimant and, if applicable, of the person representing him/her; claimant's identification document number; TIN, full address, age, gender, mobile phone number, educational qualifications and description of the facts that led to the complaint, with identification of the intervening parties; privileged interlocutor identification data for contacts with the provider; identification data of the privileged interlocutor for the purposes of contacting the ASF, which includes, in addition to the address, the respective email address. Under the IAPD, data processing also includes data from special categories (Article 9 of the GDPR), specifically data relating to health.

10. The data in question are, in general, adequate, relevant and limited to the purpose of exercising ASF's supervisory powers and for handling complaints by this entity in compliance with the principle of proportionality and data minimization provided for in paragraph c) of Article 5(1) of the GDPR.

11. However, the apparent inconsistency between the list of the customer's personal data to be processed by the insurance company or the managing entity, in the context of a claim, and the list of the complainant's personal data in the context of a relationship presented to the ASF: in the first case, the number of the civil identification document is indicated (cf. subparagraph d) of paragraph 2 of article 11 of the Project), while in the second case, the tax identification number is required (see Article 35(3)(b) of the Project). Since there is no justification for this difference regarding the personal identification data of the claimant and, especially, the reason why a citizen is identified through the NIF and not his

í

18. It is therefore important to ensure that the information on the processing of personal data provided on the websites and on the complaints management platform does not refer to the complainant's consent, nor does it depend on any act of acceptance of said information. . What may exist, if this proves necessary for the purpose of proving that the information has been provided, is the requirement of a declaration (or confirmation) that the information has become known.

19. Regarding the risk assessment, most of the identified risks are presented with a "Not significant" impact after the implementation of the mitigating measures, weighted by the probability and the impact of the same.

20. One of the risks identified by the person in charge relates to data collection through integration with the Electronic Complaints Book platform. However, the documentation provided does not detail the ways in which this integration is carried out, making it impossible to ascertain any associated risks, their probability and impact, or the measures necessary for their mitigation.

21. In turn, the documents under analysis do not detail the processing activities associated with the in-person or email collection of complaints. The AIPD only refers to electronic collection via the Consumer Portal or Electronic Complaints Book, being silent as to how this collection is carried out and how these data are stored, whether they will be included in the internal platform to follow the procedural steps, as well as how this information is eliminated at the end of the treatment.

22. It should be noted that the documents under analysis do not specify the technical details of the infrastructure, systems and applications of the solution, not allowing an assessment of whether it ensures an adequate level of data security and privacy. Little or nothing is said about the access management policy, about the backup management policy, about the protection of machines with security software (e.g., antivirus), about the access policy to databases and folders files, on the creation and management of audit records for the system that allow access and respective operations to be recorded, on security in the transport of information and on the interconnection between the various systems.

23. To that extent, the CNPD cannot accurately assess whether all risks have been identified in the IAPD, or whether others should be included, along with the respective mitigation measures.

24. In any case, taking into account that part of the infrastructure will reside on machines with a dated operating system (Windows Server 2007, with Service Pack 2), which may imply possible vulnerabilities identified and capable of being exploited by third parties, it is always recommended that the implemented solutions are installed with the latest versions (or at least recent versions) of the software,

civil identification number, the CNPD recommends reconsidering those rules, in particular, of subparagraph b) of paragraph 3 of article 35 of the Project.

12. Considering the average number of complaints analyzed, it appears that the number of data subjects involved is around 9000 per year. Thus, the high number of data subjects and the nature of the data processed call for the AIPD, under article no.

.

13. Data collection, although electronic means are preferred, can also be carried out in person. By electronic means, collection by email is foreseen, through the website of the Consumer Portal, and through integration with the digital platform of the Electronic Complaints Book.

14. It is anticipated that the personal data collected may be communicated to third parties. Under the terms of the AIPD

presented, the ASF can send the data to the entities complained of, since "the handling of the complaint implies contact with the entity to exercise the adversary system and provide the necessary clarifications". This disclosure is made through ASF's IT platform, the ASF Operators Portal, available on the internet at https://portalasf.asf.com.pt/, which allows restricted access to handle complaints.

15. Access to internal applications on the ASF network is done through authentication. Client computers are in the same domain and users authenticate with their credentials. Once authenticated in the domain, the use of applications does not require new authentication, and access is provided by defining and previously attributing authorization profiles.

16. The Consumer Portal website allows the complainant to submit a request for clarification, and to submit or consult the status of a complaint.

17. Note that when submitting a complaint, the form opens a window with information on the processing of personal data, substantiating the provisions of article 13 of the RGPD, where the person responsible is identified, the purpose and legal basis of the treatment, the rights of the holder, and the contact of the Data Protection Officer (DPD). However, it seems to follow from the IAPD (point 14) that the basis for the lawfulness of the processing is the consent of the complainant, when, strictly speaking, it is not (cf., moreover, point 18 of the IAPD, where reference is made to compliance with legal obligation). In fact, the handling of complaints by insurance companies or management entities is based on a legal obligation, being necessary for ASF to fulfill its public supervisory function.

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

for full compliance with the duty to apply "appropriate technical and organizational measures to ensure a level of security appropriate to the risk in accordance with Article 32(1) of the GDPR.

25. Regarding the risks identified by the person in charge, the CNPD considers the proposed mitigation measures acceptable. Specifically, the access profile management policies and the periodic implementation of the respective review procedures are considered adequate for the purposes in question, keeping the set of operators capable of accessing the data updated.

26. Finally, with regard to data retention periods, it should be noted that paragraph 3 of article 40 of the Draft Regulatory Standard sets a period of 5 years, without any justification being presented. . Thus, as the CNPD is not in a position to conclude that the principle of limiting the retention of personal data enshrined in Article 5(1)(e) of the RGPD has been complied with, it recommends reconsidering this aspect of the processing.

III. Conclusion

27. The analysis of the Draft regulatory rule is hampered by the omission or incompleteness of the information provided regarding some elements relating to the processing of personal data regulated therein, not allowing a full assessment of the risk arising from said processing.

28. In any case, the CNPD recalls the importance of adopting organizational and technical measures that guarantee compliance with data protection principles and the rules provided for in the RGPD, in particular in article 25 and paragraph b) of paragraph Article 32(1) of the GDPR on information security, recommending that the above observations (in particular, points 18 and 24) be taken into account.

29. The CNPD also recommends reconsidering the requirement of the NIF data to identify the claimant, in paragraph b) of paragraph 3 of article 35 of the Project (see above, points 10 and 11), as well as the deadline for data retention, set out in Article 40(3) of the Project (see above, point 26).

Approved at the session of May 18, 2022

Filipa Calvão (President)

Av.D. Carlos 1,134.1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt