NATIONAL DATA PROTECTION COMMISSION

Case No.

í

RESOLUTION/2019/605

I - Report

By court order of December 20, 2018, rendered in Case no.), was declared partially void “due to lack of reasons as to the single fine imposed, in violation of article 58, no. records to the administrative authority to supply the nullity.

The remedy of the defect referred to in the sentence obliges us, therefore, to reformulate the deliberation with regard to the grounds for the single fine imposed.

It is also important to note that, while the case is pending, Law No. 58/2019, of 8 August, the Law that ensures the implementation of Regulation 2016/679, of 27 April 2016, was approved and published (hereinafter LERGPD), which, in its article 66, revokes Law No. 67/98, of October 26 (Personal Data Protection Law - LPDP). As this law contains procedural changes in relation to the LPDP regime, it could be argued that its applicability to the present case, due to the subsidiarity of the regime provided for in article 5 of the Criminal Procedure Code (CPP), to which we must resort in matters administrative offence, either by the provisions of the revoked LPDP (cfr. article 35) or by the provisions of the new LERGPD (cfr. article 45).

It so happens, however, that the generality of the precepts of this new law do not imply, for the defendant, any improvement of his procedural situation in the specific case, since both the typification of the conducts and the framework of the fines provided for therein (cfr. articles 37 No. 1, paragraph a) and No. 2 and 38, No. 1, paragraph. i) and no. 2 of the LERGPD), or the criteria for determining the fines (cf. article 39) would not lead to different weightings by the CNPD, nor would the values specifically defined for the application of fines result in different .

The only exception to this reality is the one provided for in article 39, paragraph 3, which prescribes that “Except in the case of intent, the initiation of an administrative offense proceeding

depends on the CNPD's prior warning of the agent, for compliance with the omitted obligation or reinstatement of the violated prohibition within a reasonable period of time.”. It should, however, be borne in mind that the CNPD has already passed a resolution on the disapplication of a set of LERGPD rules (Deliberation 2019/4941), which includes the disapplication of said article (cf. point 5.3).

In the deliberation, the considerations and arguments that resulted in the judgment on the non-application of article 39, no. LERGPD would apply. However, such considerations and arguments would certainly be redounded, because there are no reasons that justify the CNPD departing from the understanding included in Deliberation 2019/494, in the non-application of this rule, as it is considered to violate European law. To that extent, it would be equally useless and meaningless to resort to the LERGPD.

Even if the applicability of the aforementioned article 39, paragraph 3, was established, since it expressly admits the initiation of an administrative offense proceeding in the event of willful misconduct, without prior warning, again the most recent regime would bring nothing useful or relevant to the specific situation of the defendant.

Added to these arguments is the jurisprudence of the Supreme Court of Justice2 on the matter of restricting the immediate applicability of criminal procedural rules, which admits it in the following terms: “I. The principle of immediate applicability of criminal procedural rules «proprio sensu» suffers from the following three restrictions: the breach of harmony and unity of the various acts (i); the appreciable and still avoidable worsening of the defendant's position, namely his rights of defense (ii); the preservation of acts validly performed in the domain of the previous law (iii)”. It follows that the possibility of breaking the harmony and unity of the various acts already practiced and the preservation of the acts validly practiced in the domain of the previous law are presented as limits that can be met by a hypothetical, but, s.m.o., not justified argument by the immediate application of the norms of the LERGPD

1 Available at https://www.cnpd.pt/bin/decisoes/Delib/DEL_2019_494.pdf.

2 BC STJ of 06-20-2012, CJ (STJ), 2012, T2, page 206.

Notwithstanding the above, there is a possibility, according to article 44, paragraph 3, of the LERGPD, that the defendant requests the exemption from the imposition of fines, however, such prerogative only operates in the face of the concrete application of a such corrective measure. However, procedurally, this means that the defendant has the possibility, even at this stage, to make the request for exemption from the application of the fine, which must be brought within 10 days, in view of the provisions of article 58, no. 3, al. a), of the RGCO.

Thus, in order to overcome the aforementioned nullity, we proceed to prepare the following resolution:

II - The National Data Protection Commission (CNPD prepared, on July 17, 2018, a draft deliberation, in which the defendant was charged with

combined provisions of Articles 5(1) al. c) and Article 5(1) al. f) with article 83, no. 5, al. a), of the General Data Protection Regulation (Regulation 679/2016, of 27 April, hereinafter RGPD), each punishable by a fine of up to €20,000,000.00 or up to 4% of turnover annual fee, whichever is the greater, as well as the commission of a foreseeable and punishable infringement under the combined provisions of Article 32(1)(b) and (d) and Article 83(1) 4, alas. a), GDPR, with a fine of up to €10,000,000.00 or up to 2% of annual turnover, whichever is higher.

The defendant was notified of the content of said bill and, pursuant to the provisions of article 50 of Decree-Law No. 433/82, of October 27, to present her defense, she came to claim (cf. pages 38 to 82) , in short, that:

1. The CNPD cannot be considered a national supervisory authority, under the terms of Article 51(1) of the RGPD, as it has not yet been formally indicated as such. To admit the opposite would violate the principle of legality enshrined in article 266 of the Constitution of the Portuguese Republic (CRP);

2. The conducts foreseen in the RGPD as punishable with the fines of article 83 are not sufficiently densified, so the intervention of the

the commission of two foreseen and punishable violations under the terms of the

national legislature is essential for them to apply, under penalty of violating the principle of typicality formulated in article 29 of the CRP;

3. Recognizes the existence of access profiles under the conditions reported in the draft deliberation of the CNPD;

4. Considers, however, that professionals with such access profiles (social action/service technicians, nutritionists, physiotherapists and psychologists) are subject to appropriate confidentiality obligations, in particular deontological ones;

5. Such professionals access relevant and necessary information for the performance of their duties;

6. The systems used do not technically allow access stratification
to information with the ideal detail, something that it understands cannot be taken from it, since it uses standardized systems by third parties, without the possibility of intervention of the mandatory use, given the determinations of the
tutelary entities;

7. It also argues that such stratification of information will tend to be impossible, since, from the outset, it is not possible to determine which specific data may be relevant for the performance of those professionals' functions;

8. Reports, however, that the latest updates made available by the Shared Services of the Ministry of Health resolved some of the issues raised by the CNPD, especially regarding the management of access credentials;

9. It also declares that it has already put into practice several of the recommendations contained in Deliberation No. 674/2018, of 17 July, of the CNPD;

10. Regarding access to the PDS (Health Data Platform), it states that “technically, a button being available to access the PDS would not mean that the user could access it, since the PDS information system is a system external to the SClinic, therefore, it must validate by itself whether the user is a doctor or nurse”;

11. Rebuts the facts that in the draft deliberation pointed to the inexistence of access logs to the SClinic system;

12. As for the accounts of active users associated with the functional group of "MEDICO", in a number much higher than the medical staff declared in the various reports and accounts, admits the possibility that some of these accounts are no longer active, although it warns of the reality of contracting of doctors in the service provision regime, which explains some of the disparity between the number of accounts and the number of professionals who actually perform functions in the

13. Assumes, even in relation to these inactive accounts, the correction of these situations, using internal technical verification processes;

14. Given the impossibility of modeling, altering or correcting the technical aspects of the systems used, it believes that it acted without fault, therefore, it is not attributable to any unlawful conduct.

He gathered eleven documents and four witnesses.

III - Appreciation

1) Regarding the alleged violation of the principle of legality due to the CNPD's arrogate to a condition that, by law, will not (yet) belong to it, it will always be said that such an argument is not valid. From the outset, and as explained in the draft deliberation, the CNPD is, for all intents and purposes, and as long as it remains unchanged, “the national authority responsible for controlling and supervising compliance with the legal and regulatory provisions in terms of protection of personal data, in strict respect for human rights and for the freedoms and guarantees enshrined in the Constitution and the law” (cf. article 22, no. by Law No. 103/2015, of August 24, hereinafter LPDP).

2) Such a provision does not only contain a desire of the national legislator to attribute to the CNPD any national matter related to the protection of personal data, but rather the distinct intention of entrusting it with any matter of this nature that is not specifically prohibited by law. And we don't see how it can violate the principle of legality.

3) Furthermore, the RGPD contains several novelties aimed at standardizing the powers of supervisory authorities throughout the European Union (EU), precisely to allow the useful effect sought by the use of this legal instrument. This concerns, for example, the possibility for any of the supervisory authorities in the EU to be equipped with adequate investigative and correction powers, thus putting an end to the disparity that reigned until the 25th of May.

4) It happens, however, that in Portugal, the CNPD has had this type of powers for a long time, and the GDPR does not constitute a relevant novelty, except for the obligations of cooperation with the other supervisory authorities of the EU, without forgetting the paradigmatic transition from heteroregulation (whose most visible face consisted of the prior assessment and authorization of the processing of personal data) to self-assessment, with the controllers and subcontractors now responsible for ensuring the legality of the processing of personal data they carry out, without there being any any intermediation by the

supervisory authorities.

5) To all these arguments, there is another one, of a merely formal nature, which is the institutional representation of Portugal that the CNPD already provides in the EU. In fact, the new European Data Protection Board, provided for in section 3 of Chapter VII of the GDPR, must, under the terms of Article 68(3) of the regulation, be “composed of the director of a supervisory authority of each Member State”. This new body of the European Union presupposes, therefore, that each country is represented by the director (or president) of each control authority of the various Member States, which, in the Portuguese case, resulted in the integration, as a full member, of the CNPD. in the CEPD, since the first meeting dated 25 May 2018.

6) As for the principle of typicality invoked by the defendant, even less seems to us to be acceptable. It will suffice, in order to remove it, to recall, from the outset, the standardizing purpose of the regulation, especially in terms of the imposition of fines, uncontroversially expressed in recital 150 of the GDPR “In order to reinforce

and harmonizing administrative sanctions for breaches of this Regulation, supervisory authorities should be empowered to impose fines. This regulation should define the breaches and the maximum amount and the criterion for setting the value of the fines resulting therefrom [emphasis added], which should be determined by the competent supervisory authority, in each individual case, taking into account all relevant circumstances of the specific situation, giving due consideration, in particular, to the nature, gravity and duration of the breach and its consequences and the measures taken to ensure compliance with the obligations contained in this Regulation and to prevent or mitigate the consequences of the breach.”

7) In addition to this reference, the Constitutional Court itself has repeatedly referred to the degree of concreteness required of norms that typify administrative offences. Paulo Pinto de Albuquerque, in his “Comment on the General Regime of Administrative Offenses”, in annotation 16 to article 2, illustrates this in an exemplary manner when he states that “the administrative offense based on the violation of general clauses (general duties of care and urbanity) and other specific obligations does not violate the principle of typicality (judgment of TC no. 338/2003, which focused on article 82, paragraph b),

of Decree-law no. 2.12). The same can be concluded from the breach of the general duty regarding the accounting organization (judgment of TC No. 455/2006, concerning article 14 of Law No. 56/98, and judgment of TC No. 198/2010 , concerning article 29 of Law No. 19/2003).".

8) Regarding the facts, it is illuminating that the defendant confirms the existence of the access profiles as described in the draft deliberation. In fact, the access credential allocation policy allowed at least 9 (nine) employees of the “TECNICO/A” functional group to enjoy the access level reserved for the “MEDICO” functional group, which translates into the indiscriminate possibility of consulting of clinical records of all hospital users.

9) Regardless of the recognition of external standardization and the availability of a specific set of types of profiles, it was the defendant who voluntarily and consciously determined that those professionals could, through profiles not suited to their functions and professional category, have indiscriminate access to the processes clinics throughout the hospital, instead of establishing other procedures, perhaps more time consuming, but certainly less intrusive of the protection of personal data that any citizen should deserve.

10) Without dispensing with this critical judgment, the arguments related to the inability to determine, a priori, which information is relevant for each of the technicians with the aforementioned access profiles, can be understood, a difficulty that is exacerbated by the architecture of the systems that do not allow the definition, step by step, or case series, of access to certain clinical information, a fact that, again, cannot be attributed to those who do not have the instruments to remedy or lessen the effects of such construction.

11) We even believe that this hypothesis removes direct intent from the defendant's conduct, makes the necessary intent questionable, but does not in any way preclude the existence of eventual intent. So much so, that the defendant confesses to having always proceeded with knowledge of the existence of these system insufficiencies, not refraining, however, from continuing to grant undue access privileges to a group of professionals who should never be able to indiscriminately access the clinical files of clients.

12) It is unsustainable to defend that any social worker can access the entire clinical file of the client in order to perform his/her function, and such a defense is even more untenable if access in this manner is possible without time limit.

13) As equally indefensible is the existence of access credentials that allow any doctor, of any specialty, at any time to access

the data of the clients of a specific hospital. The beginning

of data minimization and the principle of “need to know” (or, in the Anglicism "needto knoW'), prohibit or intend to prohibit the collection, but also the access and other processing of unnecessary information for the intended purpose.

14) For all these reasons, the CNPD cannot admit that the technical limitations pointed out can justify the unrestricted adoption of access validation procedures that practically make the essential core of the fundamental right to the protection of personal data irrelevant.

15) The defendant's allegation, which points to a much greater restriction of the access profiles of non-medical professionals who have the profiles of the functional group “TECHNICIAN” and activity group “MEDICO” is clearly reductive since, even if such restrictions exist, they were not enough to prevent the CNPD technicians from seeing a test user created by the SSI of the defendant (precisely from the “TECHNICIAN” functional group and “MEDICO” activity group) that allowed them to “search for users registered in that hospital without restrictions and that he had permission to access all the elements that make up the clinical process of these users”, as stated in the report attached to the draft deliberation (cf. page 6).

16) By knowingly allowing professionals from different categories to have access to unrestricted information about the clinical process of clients of the ^^^B, the defendant did not take any care to ensure compliance with that principle, having, moreover, circumvented a limitation of the systems that had been adopted for security and privacy reasons.

17) In addition, according to her own defense, the defendant will never take care to intercede with the SPMS in order to correct this aspect of the system which, as the recent update demonstrates, should and could be changed in advance.

18) Regarding the possibility of accessing unnecessary or relevant information allowed by these profiles, the inspection team verified and collected proof of access to the PDS from the test user account. In fact, as far as it was possible to verify in the inspection context, the PDS platform does not validate the user's authentication, thus explaining that it was possible to access

the PDS with a "TEST USER", which had no associated mechanographic number or number. order (doctor or nurse).

19) Contrary to the argument of^^^I, it is up to hospital centers and other health care institutions to correctly validate the user and identify the corresponding profile, not the PDS.

20) As for the maintenance of useless profiles concerning medical professionals who no longer provide services to the person who has not taken care to eliminate, the judgment of censorship remains unchanged.

21) Remember that, of the 18 (eighteen) user accounts that the CNPD found to be effectively deactivated, only one corresponded to a medical professional.

22) Assuming that this conduct has not caused concrete damage to the protection of personal data of the clients of that hospital, one cannot, however, ignore or disregard the breach of objective duties of those responsible for the treatment, especially when the potential access to special categories of data, a concept specified in Article 9(1) of the GDPR, such as health data.

23) It should be noted that the defendant did not deny the existence of such profiles, limiting herself to claiming that some (few or many) of them are due to the hiring, under a service provision regime, of doctors who are only performing functions transiently in the ^^H. The concrete and rigorous lack of knowledge of the

universe of access accounts that should have been eliminated is a good demonstration of the lack of a reliable auditing system.

24) Equally objectionable is the procedure for creating accounts which, contrary to what has been argued, is not even fully controlled by the administration of^^^B

25) In fact, evidence was collected in the context of an inspection that demonstrates that the account creation process is not always governed by the procedure referred to by the defendant. Annex I (of pages 9) presents the transcript of e-mails exchanged between the Coordinator of the Physiotherapy sector of the

the Clinical Pathology Department and the Information Systems Service (SSI), which expressly determine the request for the creation of user accounts, without any pronouncement on the part of the administration of the^^H-

26) Even though it is admitted that the defendant started a path to correct this situation, the fact is that, at the time of the inspection, the creation of accounts did not minimally respect the principles of the GDPR.

27) Regarding the absence of access LOGS, it is confirmed that the IT technician exported the table «sys_log_acessos» with the name «log_acessos_assistant_social.XLS», which displays what appear to be input and output events of a system. It is assumed that they are associated with accesses to SCiínico, although this information has not been confirmed.

28) From an auditability point of view, the input and output logging in an application provides very limited information about its use. The CNPD recognizes, however, that the inclusion of a higher level of activity registration is dependent on changes in the application logic and that these changes will only be within the reach of the entity that develops the software - in this case the SPMS.

THE

29) Compliance with the recommendations of the CNPD, registered in Deliberation no. 674/2018, of 17 July, which are intended precisely to correct elements considered critical or of substantive relevance, is positively highlighted.

30) It is recognized that there are updates to the systems provided by the SPMS that follow the correct path, although potentially not complete, in accordance with the rules of the RGPD.

The witnesses presented were not heard as the matter of fact was generally confirmed and, as for the undisclosed contested facts, they do not require further clarification or contradictory, which results in any testimonies being irrelevant to the discovery of the material truth.

Bearing in mind the defense presented by the defendant and the critical judgment made on her by the CNPD, some of the facts are altered in light of the information and clarifications provided therein.

IV - With the elements contained in the records, of interest for the decision, we consider the following to be proven:

facts

1. On July 2, 2018, the National Data Protection Commission conducted an inspection of the management systems and access to information at the premises of 2 3

2. In the context of this inspection, it was found that there was no document that provided for the correspondence between the functional skills of users and the profiles of access to information, namely clinical information, or where the criteria that allow such correspondence to be made are listed.

3. It was also verified the absence of any document defining the rules regarding the procedure for creating an account for users of the Hospital's information system;

Process no.'

7

NATIONAL COMMISSION

DF DATA PROTECTION

4. Furthermore, the determination of the creation of user accounts and information access profiles is communicated by e-mails addressed to the Information Systems Service (SSI) originating from service managers and other professionals;

5. This procedure is under review and correction.

6. uses the Integrated Hospital Information System (SONHO) and the hospital clinical record system (SClinic), applications provided by the Shared Services of the Ministry of Health, EPE (SPMS); the first is used for administrative support of the hospital and the second records the clinical information of users, allowing access, use and sharing of this information between health professionals;

7. Has the processing of personal data from the systems of

information SONHO and SAM (previous name of the SClinic application)3.

8. In the SONHO application, each user account has two attributes that allow hospital services to manage the system's access profiles; the functional group and the activity group, assigning them codes; the functional group distinguishes the various functional areas that exist in a hospital environment (e.g. “ADMINISTRATIVE/A”, “TECHNICIAN/A”, “DOCTOR”, “INFORMATICS”, “AUXILIARY”), while the activity group allows to distinguish different areas within of a functional group (e.g., in the functional group of “DOCTOR”, there is “SURGEON”, “ANESTHESIST” and “DOCTOR”);

9. There is a functional group called “TECHNICIAN/A”, which includes different activities - “NUTRITIONIST”,

“PHYSIOTHERAPIST”, “PSYCHOLOGIST” and “SOCIAL SERVICE” (cf. Annex I);

10. The functional group “MEDICO” corresponds to code 5;

11. The functional group “TECNICO/A" corresponds to code 2;

12. 10 professionals from the “SOCIAL SERVICES” area of activity are registered in the CHBM SONHO information system (cf. Annex II);

13. These 10 professionals have associated code 2, which corresponds to the functional group of “TECNICO/A”; 3

3 Authorizations no.^H/2012 and no.^H/2012, respectively, issued by the CNPD no| 2012 and on the same date notified to the^^H.

in

14. Of these 10 professionals, 9 also have code 5 associated with them, which corresponds to the functional group of “MEDICO” (cf. Annex III);

15. Non-medical professionals associated with code 5 have, through this code and profile, access permissions to the entire clinical process of all hospital users, through the SClinic system;

16. On the initiative of the CNPD, a test user account was created (with the name “UTILIZADOR TESTE”) with the profile identical to that of the 9 technicians of the Social Service - with code 2 and 5 - and it was verified that it allowed the access, without any restrictions, to the clinical file of ^^Hi users, which includes the diagnosis, the results of the auxiliary diagnostic means and other information recorded in the clinical file of each user (cf. Annex IV);

17. Still within SClinico, with the same user account (with

TECHNICIAN/A- SOCIAL SERVICE), access, via the Health Data Platform, as this allows it, to the information residing in another hospital of the National Health Service regarding clinical episodes

associated with a user of the ^^^I (cf. Annex V);

18. In point 4 of authorizations No.^^B/2012 and ^^Bí2012, under the heading Security Measures, the CNPD expressly

determined the need for the person in charge to adopt mechanisms for identifying and authenticating users, as well as managing profiles of access;

19. The information systems provided by the Shared Services of the Ministry of Health, EPE (SPMS) do not allow users to define their own parameters, namely in terms of access profiles.

20. There are 985 active users associated with the “MEDICO” functional group, in

21. Item 5 ("Human Resources") of the report and accounts of|

on the map of

staff registered there, on page 33, the existence of 280 doctors;

22. The human resources plan, on page 14 of the Activities Plan for 2018 of the same hospital (available at

points to the existence of 296

doctors at the service of the said EPE, this year.

23. The

recognized the existence of unused profiles, although safeguarding the

reality of service provision contracts, which result in the creation of temporary profiles of doctors hired under this regime, failing to quantify the phenomenon.

24. There are only 18 inactive user accounts (15 technicians, 1 pharmacist and 1 doctor), with the most recent inactivation dated 11/11/2016 (cf. Annex VI);

25. In point 4 of authorizations No.^^B/2012 and M/2012, under the heading Security Measures, the CNPD expressly determined, in subparagraph c), the need for the

26. The defendant acted deliberately, knowing that she was obliged to apply the technical and organizational measures essential for the identification and authentication of users, as well as for the management and delimitation of their information access profiles, stratifying them according to the different privileges of access corresponding to the professional categories of

its workers, and also the guarantee of information security, in addition to having a reliable auditing system of such identifications, accesses and security guarantees.

27. The defendant acted freely, voluntarily, knowingly and knowing that her conduct was as prohibited and punished by law

V - Reasoning of the decision in fact

The facts given as established resulted:

- From the inspection report on pages 4 to 10, which describe the circumstances in which the information access systems operated and the specific conditions of access, allowing professionals with profiles improperly assigned to access the clinical information of all the defendant's clients and not taking care to guarantee the minimum conditions system auditability and security;

- Of the defendant's written defense, on pgs. 38 to 82, which recognize the shortcomings detected regarding the procedures for defining accounts and access privileges, regarding the inability to determine restrictions on access to information according to the specific function of the employees of the

have a reliable audit system

CHBM and regarding the non-compliance with the duties of monitoring unused accounts and their elimination.

VI - It is verified, in the light of the verified facts, that it appears to be sufficiently

two offenses foreseen and punishable under the combined provisions of the

" article 5, no. 1 al. c) - violation of the principle of data minimization, allowing indiscriminate access to an excessive set of data by professionals who should only have access to them in specific and previously justified cases; and article 83, no. 5, al. a) - violation of the basic principles of processing, of the General Regulation on Data Protection (Regulation 679/2016, of 27 April, hereinafter RGPD); as well as of the

■ article 5(1) al. f) — violation of the principle of integrity and confidentiality, due to the non-application of technical and organizational measures aimed at preventing illicit access to personal data; and Article 83(5) al. a) - violation of the basic principles of treatment, of the General Regulation on Data Protection (Regulation 679/2016, of 27 April, hereinafter RGPD),

each punishable by a fine of up to € 20,000,000.00 or up to 4% of annual turnover, whichever is higher.

Likewise, the practice, by the same defendant, of a foreseen and punishable offense under the combined provisions of - article 32, paragraph 1, b) and d) - incapacity of the person responsible for treatment to ensure the confidentiality, integrity, availability and permanent resilience of treatment systems and services, as well as the failure to apply appropriate technical and organizational measures to ensure a level of security appropriate to the risk, namely a process to test, assess and evaluate regularly the effectiveness of technical and organizational measures to ensure the security of treatment; and Article 83(4) al. a), GDPR, with a fine of up to €10,000,000.00 or up to 2% of annual turnover, whichever amount is higher.

indictment of the practice by the defendant

of two administrative offenses for the practice of

NATIONAL COMMISSION

DATA PROTECTION

Case No.

9

In accordance with the provisions of Article 83, paragraph 1, s. a) to k), 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 or purpose of the data processing in question, as well as the number of data subjects affected and the level of damage suffered by them - we are faced with two offenses punishable with the most serious frame provided for by the GDPR and an offense punishable with the least serious frame of that regulation, given that, at least, since May 25, 2018, both offenses have been committed. The number of cardholders affected corresponds to the universe of customers of the

precise number of customers difficult to quantify, the Access Report related to

a number in the tens of thousands. It is also relevant, at this point, to point out that we are dealing with health data, which fall into the special categories of data, which considerably increases the risk of damage to data subjects;

■ The intentional or negligent nature of the infraction - the conduct related to the detected infractions is considered to be malicious, even if as an eventual intent, since the defendant represented the practice of the infraction as a possible consequence of the conduct and was satisfied with it .

- The initiative taken by the controller or the processor to mitigate the damages suffered by the data subjects - the conduct of the defendant who adopted, from the moment of the inspection, the appropriate measures to rectify the weaknesses detected, which are present or already implemented or in the implementation phase

■ The degree of liability of the controller or processor, taking into account the technical or organizational measures implemented by them under the terms of articles 25 and 32 - the defendant is considered to be responsible for violating the restrictions of the levels of access of professionals to the personal data of the clients, since it consciously allowed to associate the

rV process

9v

f

functional group of "PHYSICIAN" which should only be accredited with a "TECHNICIAN" profile; As for the lack of procedures to verify the need to maintain the access profiles of doctors who are no longer at the service of the service, one cannot fail to consider a degree of responsibility

equally high on the part of the defendant, since it was her sole responsibility to ensure the control of the need and elimination of these profiles, namely through appropriate audit procedures.

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

■ The degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate its possible negative effects - which is considered appropriate, not only in the face of correcting the shortcomings detected, but also in complying with the content of Deliberation n. 674/2018, of July 17;

■ The specific categories of personal data affected by the infringement - special categories of personal data, in accordance with Article 9(1) of the GDPR, as well as other non-sensitive information, such as customer identification. These data allow the identification of their holders and the improper access allowed with the conduct of the defendant constitutes a serious interference in their privacy;

B How 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 - the infringements being known through media reports and subsequently confirmed in the

inspection carried out by the CNPD;

■ Compliance with the measures referred to in article 58.a, paragraph 2, if they have been previously imposed on the controller or processor in question in relation to the same matter - this criterion not being applied, since there were no any predetermined corrective measures;

■ Compliance with codes of conduct approved under the terms of article 40 or certification procedure approved under the terms of article 42 - criterion that also does not apply, as there is no code of conduct or certification procedure, under the terms mentioned ;

and

■ Any other aggravating or mitigating factor applicable to the circumstances of the case, in light of Article 83(2)(k) of the GDPR, such as the financial benefits obtained or the losses avoided, directly or indirectly, through the infringement -relevant here, as a factor

the aggravating factor, as to the infringement relating to the violation of article 32, no. 1, subparagraphs b) and d) - the existence of prior authorizations from the CNPD where, under the heading Security Measures, the CNPD expressly determined the need for the have an audit system

reliable, and the defendant cannot be unaware of this obligation; mitigating factor, the circumstance that the parameters for monitoring the LOGS of access to the SClínica's information do not depend on the defendant, but rather on the SPMS.

■ Application of the fine

Bearing in mind the aforementioned criteria, the CNPD considers it necessary to impose, in the specific case, a fine on the defendant, considering that this is the effective proportionate and dissuasive measure that is imposed given the specific circumstances in which the infringements occurred.

As expressed in the draft determination, the fine frame abstractly applicable to the defendant for the foreseen and punishable offenses under the combined provisions of Articles 5(1) al. c) and Article 5(1) al. f) with Article 83(5) al. a), of the General Data

Protection Regulation (Regulation 679/2016, of 27 April, hereinafter RGPD), each punishable by a fine of up to €20,000,000.00 or up to 4% of annual turnover , whichever is higher, as well as the commission of an infringement, in competition, foreseen and punishable under the combined provisions of Article 32(1)(b) and d) and Article 83(n) 4, al. a), GDPR, with a fine of up to €10,000,000.00 or up to 2% of annual turnover, whichever amount is higher.

However, after consulting the defendant's report and accounts for the year 2017

a result is observed

net of 16.^HI^IH€ (sixteen million

This means that the specific framework of the fines to be

Case No. 1

10v

/

apply are set, in the first case, between €0.00 and €20,000,000.00 and, in the second case, between €0.00 and €10,000,000.00.

Valuing the facts found in the light of the above mentioned criteria, the CNPD,

- pursuant to Article 58(2) al. b) of the GDPR, it considers that the application of two fines to the defendant, each one in the amount of € 150,000.00 (one hundred and fifty thousand and euros) for the practice of two foreseen and punishable offenses under the combined provisions of articles 5, no. 1 al. c) and 5th, no. 1, al. f), all of the aforementioned regulation;

pursuant to Article 58(2) al. i) of the RGPD, the imposition of a fine of € 100,000.00 (one hundred thousand euros) on the defendant for the practice of the foreseen and punishable offence, in accordance with the combined provisions of Articles 32(1)(b) and d) and Article 83(4) al. a), all of the aforementioned regulation.

Once the partial penalties are framed, it is verified, according to article 83, paragraph 3 of the RGPD, that, in case of violation of several provisions of the regulation by the person responsible, “the total amount of the fine cannot exceed the amount specified for the most serious breach”, in this case, €20,000,000.00 (twenty million euros), constituting the abstractly applicable maximum limit.

Article 19(3) of the General Regime for Administrative Offenses also provides, applicable in the alternative, ex w article 35 of

Law No. 67/98, of 26 of , that “The fine to be imposed it cannot be less than the highest of the fines specifically applied to the various offences.”, ie € 150,000.00.

- We have, therefore, that the abstract frame of the single fine to be applied is between a minimum of €150,000.00 (one hundred and fifty thousand euros) and a maximum of 20,000,000.00 (twenty million euros).

- Justification for the application of the single fine

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

In this sense, in order to proceed with the legal overlap, it is necessary to verify the following requirements, of a procedural and material nature, i) that they are sanctions

relating to administrative offenses committed before the final sentence of the conviction by any of them, ii) that have been committed by the same defendant and that the partial sanctions are renewed in the same type.

What is cumulatively verified in the present case, due to the existence of the effective or pure contest, in the real contest aspect, given the existence of a plurality of infractions practiced in the terms described above, corresponding to the plurality of actions in question, by the defendant .

It was found that the defendant acted deliberately, refraining from applying the technical and organizational measures necessary for the identification and authentication of users, as well as the management and delimitation of their information access profiles, stratifying them according to the different privileges. of access corresponding to the professional categories of its workers, and also the guarantee of information security, in addition to having also refrained from implementing a reliable audit system of such identifications, accesses and security guarantees. Such conduct is particularly objectionable, as the personal data in question relate to special categories of data, which are themselves subject to additional protection under Article 9 of the GDPR. Equally serious is the fact that the violations relate to the entire universe of data holders who are clients of that hospital.

Considering that the defendant acted freely, voluntarily and consciously, representing the practice of administrative offenses as a possible consequence of her conduct and conforming to this, she believes that a sanction is due to reflect the high censorship of this behavior, even though she recognizes the subsequent efforts investigation actions in order to correct the violations found In the consideration made to decide on the single fine to be imposed, and without prejudice to the high degree of censorship of the defendant's conduct, the CNPD considers relevant the fact that the defendant does not have a history of application of administrative offenses for breaching data protection rules, as well as the fact that any data breaches or other data processing operations that have significantly affected data subjects have not been specifically determined, which precludes the imposition of minimal fines close to the abstractly applicable maximum limit, combined with the circumstances ances that were found, in what

Process no.'

r

O

11V

concerning the subjective imputation of the defendant, and also taking into account the legal interests protected by the administrative offenses in question, which she committed, it appears effective, proportionate and dissuasive, to apply to the defendant:

In legal terms, under the combined provisions of article 83, paragraph 3 of the RGPD and 19, paragraph 3 of the RGCO, a single fine of € 380,000.00 (three hundred and eighty thousand euros).

VII - Conclusion

In view of the above, the CNPD resolves: Apply to the mÉÈÊSSBÈ

watching the

provided for in paragraph 3 of article 83 of the RGPD, a single fine, in the amount of € 380,000.00 (three hundred and eighty thousand euros) due to the violation of the principles of data minimization and integrity and confidentiality, as well as breach of the obligation to apply appropriate technical and organizational measures to ensure a level of security appropriate to the risk, namely, a process to regularly test, assess and evaluate the effectiveness of technical and organizational measures to ensure

the security of processing.

Pursuant to articles 58, paragraphs 2 and 3 of the General Regime for Administrative Offenses, inform the defendant that:

a) The conviction becomes final and enforceable if it is not judicially challenged, under the terms of article 59 of the same diploma;

b) In the event of a judicial challenge, the Court may decide by means of a hearing or, if the defendant and the Public Prosecutor do not object, by means of a simple order.

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

NATIONAL DATA PROTECTION COMMISSION

Case No.

Approved at the plenary meeting of November 26, 2019

Pedro Mourão

Teresa Naia

José Grazina^Mach

Filipa Calvão (President)