Process No. 9932/2018 1

t

NATIONAL COMMISSION

DATA DEPROTECTION

DELIBERATION No. 984/2018

I - The National Data Protection Commission (CNPD) prepared, on July 17, 2018, a draft resolution, in which the defendant was charged

combined provisions of Articles 5, paragraph 1 al. c) and article 5, no. 1 al. f) with article 83, no. 5, par. a), of the General Data Protection Regulation (Regulation 679/2016, of April 27, hereinafter RGPD), punishable, each of them, with a fine of €0.00 to €20,000,000.00 or up to 4% of the annual turnover, whichever amount is higher, as well as the commission of a breach foreseen and punishable under the terms of the combined provisions of article 32, paragraph 1, subparagraphs b) and d) and article 83. , No. 4, al. a), of the GDPR, with a fine of €0.00 to €10,000,000.00 or up to 2% of annual turnover, whichever amount is higher.

Once the defendant was notified of the content of the said project 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 (cfr. pages 38 to 82) , in short, that:

1. The CNPD cannot be considered as a national supervisory authority, under the terms of article 51, paragraph 1 of the RGPD, as it has not yet been formally indicated as such. Admitting otherwise would violate the principle of legality contained 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 that the intervention of the national legislator is indispensable for them to apply, under penalty of violation of 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 these access profiles (social action/service technicians, nutritionists, physiotherapists and psychologists) are subject to

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

Tel: 213 928400

Fax: 213 976 832

PRIVACY LINE

Weekdays from 10 am to 1 pm

doubts@cnpd.pt

www.cnpd.pt

THE

adequate confidentiality obligations, namely deontological ones;

5. Such professionals have access to 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 he understands cannot be attributed to him since he uses systems standardized by third parties, without the possibility of intervention by and of mandatory use, given the determinations of the guardianship entities;

7. It also argues that such a 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. Informs, however, that the latest updates made available by the Shared Services of the Ministry of Health have 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 July 17, of the CNPD;

10. Regarding access to the PDS (Health Data Platform), he declares 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 an external system to the SClínico, therefore, it must validate itself if the user is a doctor or nurse";

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

12. As for the accounts of active users associated with the "MEDICO" functional group, in a much higher number than the

medical staff declared in the various reports and accounts, it admits the possibility that some of these accounts are no longer active, although it warns of the reality of contracting of doctors under the provision of services, which explains some of the disparity between the number of accounts and the number of professionals who effectively perform functions in the

I

V

NATIONAL COMMISSION

DATA PROTECTION

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

14. Given the impossibility of modelling, altering or correcting the technical aspects of the systems used, he understands that he acted without fault, therefore, no illicit conduct is attributable to him.

He gathered eleven documents and four witnesses.

II - Assessment

1) Regarding the alleged existence of violation of the principle of legality due to the CNPD assuming a condition that, by law, will not (yet) belong to it, it will always be said that such an argument is unfounded. From the outset, and as explained in the draft decision, the CNPD is, for all intents and purposes, and as long as this is not changed, “the national authority whose attribution is to control and supervise compliance with the legal and regulatory provisions on the protection of of personal data, in strict respect for human rights and for the freedoms and guarantees enshrined in the Constitution and in the law” (cf. article 22, no. 1 of Law no. 67/98, of 26 October, amended by Law No. 103/2015, of August 24, hereinafter LPDP).

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

3) In addition, the RGPD contains several innovations tending to standardize the powers of the control 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 of any of the control authorities in the EU being equipped with adequate powers of investigation and

correction, thus ending the disparity that reigned until the 25th of May.

Rua de São Bento, 148-3° • 1200-821 LISBOA

Tel: 213 928400 Fax: 213 976 832

www.cnpd.pt

21 393 OO 39

PRIVACY LINE

Weekdays from 10 am to 1 pm

doubts@cnpd.pt

4) However, in Portugal, the CNPD has had this type of power for a long time, and the relevant GDPR is not new, except in terms of cooperation obligations with other EU supervisory authorities, without forgetting the paradigmatic transition from hetero-regulation (whose most visible face consisted of the prior assessment and authorization of personal data processing) to self-assessment, with those responsible for processing and subcontractors now being responsible for ensuring the legality of the processing of personal data that they carry out, without any any intermediation by the supervisory authorities.

5) In addition to all these arguments, there is another, of a purely formal nature, which is the institutional representation of Portugal that the CNPD already ensures in the EU. Indeed, the new European Data Protection Board, provided for in Section 3 of Chapter VII of the RGPD, 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, then, that each country is represented by the director (or president) of each control authority of the various Member States, which, in the case of Portugal, resulted in the integration, as a full member, of the CNPD in CEPD, since the first meeting dated May 25, 2018.

6) As for the principle of typicality invoked by the defendant, it seems to us to be even less applicable. It will suffice, in order to rule it out, to recall, from the outset, the standardizing purpose of the regulation, particularly in terms of the application of fines, uncontroversially expressed in recital 150 of the RGPD “In order to reinforce and harmonize administrative sanctions for violations of this regulation, the authorities supervisory bodies should be empowered to impose fines. This regulation should define the violations and the amount

maximum and the criteria for setting the value of fines arising therefrom [underlined

our], which shall be determined by the competent supervisory authority, in each individual case, taking into account all the relevant circumstances of the specific situation, duly considering, in particular, the nature, gravity and duration of the breach and its consequences and the measures taken to ensure compliance with the obligations set out in this Regulation and to prevent or mitigate the consequences of the infringement.".

7) In addition to this reference, the Constitutional Court itself has repeatedly referred to the degree of concreteness required of norms that typify administrative offenses. Paulo Pinto de Albuquerque, in his "Commentary on the General Regime of Administrative Offenses", in annotation 16 to article 2, illustrates this exemplarily when he refers 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. 422/89, of 2.12). The same can be concluded from the violation of the generic duty regarding the accounting organization (CA decision No. 455/2006, regarding article 14 of Law No. 56/98, and TC judgment No. 198/2010 , relating to Article 29 of Law No. 19/2003).".

8) Regarding the facts, it is clarifying that the defendant confirms the existence of the access profiles as described in the draft decision. Indeed, the policy for assigning access credentials allowed at least 9 (nine) employees of the "TECHNICIAN/A" functional group to enjoy the access level reserved for the "MEDICO" functional group, which translates into the indiscriminate possibility of consulting of clinical files of all hospital users.

9) Regardless of recognizing the external standardization and availability of a determined 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 hospital-wide clinicians, rather than establishing

other procedures, perhaps more time consuming, but certainly less intrusive to the protection of personal data that any citizen deserves.

10) Without disregarding this critical judgment, one can understand the arguments related to the inability to determine, a priori, what information is relevant for each of the technicians with the aforementioned access profiles, a difficulty that is exacerbated by the architecture of the systems that do not allow the definition, step by step or casuistry 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 the direct intent of the defendant's conduct, makes the necessary intent questionable, but does not preclude, in any way, the existence of eventual intent. So much so, that the defendant confesses to having always acted with knowledge of the existence of these shortcomings in the system, not refraining however from continuing to attribute undue access privileges to a group of professionals who should never be able to indiscriminately access clients' clinical files.

12) It is unsustainable to defend that any social worker can access the entirety of the client's clinical file in order to be able to carry out his or her function, and such a defense is even more unsustainable if access in these ways is allowed without a time limit.

13) Equally indefensible is the existence of access credentials that allow any doctor, of any specialty, at any time to access customer data from a given hospital centre. The principle of data minimization and the principle of “need to know” (or, in the Anglicism “need to know”), prohibit or intend to prohibit the collection, but also access and other processing of unnecessary information for the intended purpose.

f:

7

NATIONAL COMMISSION

DATA DEPROTECTION

14) For all these reasons, the CNPD cannot admit that the technical limitations mentioned 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 restrictiveness of the access profiles of non-medical professionals who have the profiles of the functional group "TECHNICIAN" and activity group "MEDICO" is manifestly reductive since, even if such restrictions exist, they were not enough to prevent the CNPD technicians from even seeing a test user created by the defendant's SSI (precisely from the functional group "TECHNICIAN" and activity group "MEDICO") that allowed them to "search for users registered in that hospital institution without restrictions and that he had access permission to all the elements that make up the clinical file of these users", as stated in the report attached to the draft deliberation (cfr. page 6).

16) By knowingly allowing professionals from different categories to

access to unrestricted information about the clinical process of clients of a

defendant did not take the slightest care to ensure compliance with that principle, having, moreover, circumvented a limitation of the systems that had been adopted for reasons of security and privacy.

17) Added to this is that, according to her own defense, the defendant will never be careful 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) As regards the possibility of accessing information that is not necessary or relevant permitted by these profiles, the inspection team verified and collected proof of access to the PDS from the user account of

test. In fact, as far as it was possible to verify in the context of inspection, 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 not associated any mechanographic number or number order (from a doctor or nurse).

19) Contrary to the argument that it is up to hospital centers and

other health care institutions carry out the correct user validation and identification of the corresponding profile, not the PDS.

20) Regarding the maintenance of useless profiles concerning medical professionals

that no longer provide services to and that the latter did not take care to eliminate, the judgment

censorship remains unchanged.

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

22) Assuming that this conduct did not cause concrete damage to the protection of personal data of the clients of that hospital center, one cannot, however, ignore or disregard the breach of objective duties of those responsible for the treatment, especially when it is in question 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 arguing that some (few or many) of them are due to the hiring, under a service provision regime, of doctors who are only performing functions temporarily no. 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 alleged, is not even fully controlled by the administration of the

25) Indeed, evidence was collected in the context of an inspection that demonstrates that the process of creating accounts is not always governed by the procedure referred to by the defendant. Annex I (page 9) presents the transcription of e-mails exchanged between the Coordinator of the Physiotherapy Sector of

the Directorate of Clinical Pathology 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

26) Even if it is accepted that the defendant embarked on 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 RGPD.

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

28) From an auditability point of view, logging in and out of 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.

Rua de São Bento, 148-3°

Phone: 213 928400

www.cnpd.pt

1200-821 LISBOA Fax: 213 976 832

PRIVACY LINE

Weekdays from 10 am to 1 pm

doubts@cnpd.pt

29) Compliance with the recommendations of the CNPD, included in Deliberation No. 674/2018, of July 17, is positively

highlighted, which are precisely intended to correct elements considered critical or of substantive relevance.

30) It is recognized that there are updates to the systems provided by the SPMS that follow the correct course, even if potentially not complete, in accordance with the GDPR rules.

The witnesses presented were not heard since the factual matter was generally confirmed and, as for the disputed facts not revealed, they do not require further clarification or contradictory, which results in the eventual testimonies being irrelevant for the discovery of the material truth.

In view of the defense presented by the defendant and the critical judgment that the CNPD made about her, some of the facts are changed in light of the information and clarifications provided therein.

III - With the elements contained in the case file, of interest to the decision, we consider the following to be proven:

Facts

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

2. In the context of this inspection, it was verified that there is no document where the correspondence between the functional competences of the users and the profiles of access to information, namely clinical information, is foreseen, or where the criteria that allow such correspondence are listed.

3. It was also verified that there was no document containing

defined the rules relating to the procedure for creating user accounts in the information system of ;

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 currently being revised and corrected.

6. uses the Integrated Hospital Information System (SONHO) and the

hospital clinical record (SClínico), applications made available by the Shared Services of the Ministry of Health, EPE (SPMS);

the first is used for hospital administrative support and the second records the clinical information of users, allowing access, use and sharing of this information between health professionals;

7. The processing of personal data from the systems of

SONHO and SAM information (previous designation of the SClínico application)1.

8. In the SONHO application, each user account has two attributes that allow hospital services to manage access profiles to the system: the functional group and the activity group, assigning codes to them; the functional group distinguishes the various functional areas that exist in a hospital environment (e.g., “ADMINISTRATIVE/A”, “TECHNICIAN/A”, “MEDICAL”, “INFORMATICS”, “ASSISTANT”), while the activity group allows distinguishing different areas within a functional group (e.g., in the functional group of “DOCTOR”, there are “SURGEON”, “ANANESTHESIST” 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 “MEDICO” functional group corresponds to code 5;

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

12. 10 professionals in the area are registered in the SONHO information system

“SOCIAL SERVICE” activity (cf. Annex II);

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

Rua de São Bento, 148-3° Tel: 213 928400

1200-821 LISBOA Fax: 213 976 832

www.cnpd.pt

PRIVACY LINE

Weekdays from 10 am to 1 pm

doubts@cnpd.pt

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

15. Non-medical professionals who are 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 (named “USER TEST”) with a profile identical to that of the 9 Social Service technicians - with code 2 and 5 - having been verified that it allowed the access, without any restrictions, to the clinical file of users of , which contains 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 SClínico, with the same user account (with the profile of TECHNICIAN/A - SOCIAL SERVICE), access was made via the Health Data Platform, as this allows it, to information residing in another hospital in the National Health Service relating to clinical episodes associated with a user

do (cf. Annex V);

18. In point 4 of authorizations no. 5795/2012 and 5796/2012, 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 access profiles ;

19. The information systems made available 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 functional group "MEDICO", in ;

21. Point 5 (“Human Resources”) of the report and accounts of the

2017 (available at

, indicates, on the staff map

inscribed there, on page 33, the existence of 280 doctors;

22. The human resources plan, on page 14 of the Activity Plan for 2018 of the same hospital

points to the existence of 296 physicians

at the service of said EPE, this year.

23. acknowledged the existence of unused profiles, while 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), the most recent inactivation being dated 11/11/2016 (cf. Annex VI);

25. In point 4 of the authorizations, under the heading Measures of

Security, the CNPD expressly determined, in paragraph c), the need for the

26. The defendant acted deliberately, well aware that she was obliged to apply the technical and organizational measures essential to the identification and authentication of users, as well as the management and delimitation of their information access profiles, stratifying them according to different privileges corresponding to the professional categories of its workers, and also the guarantee of information security, in addition to having a reliable audit system of such identifications, accesses and security guarantees.

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

IV - Motivation of the factual decision The facts considered established resulted in:

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

- From the written defense of the defendant, on pages 38 to 82, where the detected shortcomings are recognized regarding the procedures for defining accounts and access privileges, regarding the inability to determine restrictions on access to information according to the specific role of the employees of the

have a reliable audit system.

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

V - It is verified, in view of the verified facts, that the practice by the defendant of two administrative offenses for the practice of two offenses foreseen and punishable under the terms of the combined provisions of the

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

as well as the

• article 5, no. 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, no. 5, par. a) - violation of the basic principles of processing, of the General Regulation on Data Protection (Regulation 679/2016, of April 27, hereinafter RGPD), punishable, each of them, with a fine of €0.00 to €20,000,000.00 or up to 4% of the

annual turnover, whichever amount is higher.

It is also shown that the practice, by the same defendant, is sufficiently indicted

of an offense envisaged and punishable under the terms of the combined provisions of the

• article 32, paragraph 1, points b) and d) - inability of the controller to ensure the confidentiality, integrity, availability and permanent resilience of the treatment systems and services, as well as the non-application

appropriate technical and organizational measures to ensure a level of security appropriate to the risk, in particular a process

for regularly testing, appraising and evaluating the effectiveness of technical and organizational measures to guarantee the security of the processing; and article 83, no. 4, par. a), of the GDPR, with a fine of €0.00 to €10,000,000.00 or up to 2% of annual turnover, whichever amount is higher.

H

In accordance with the provisions of article 83, paragraph 1, ais. a) to k), the determination of the measure of the fine is made according to 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 RGPD and an offense punishable with the least onerous frame of this regulation, given that, at least, since May 25, 2018, both offenses have been committed. The number of holders affected corresponds to the universe of clients of , that is, of the two hospitals that comprise it, the

Being the

precise number of customers difficult to quantify, the Access Report for ,2017

makes it possible to extrapolate

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

• The intentional or negligent nature of the infraction - the conduct related to the detected infractions is considered to be intentional, even if by way of possible deceit, since the defendant represented the practice of the offense as a possible consequence of the conduct and accepted it .

Rua de São Bento, 148-3° • 1200-821 LISBOA

Tel: 213 928400 Fax: 213 976 832

www.cnpd.pt

PRIVACY LINE

Weekdays from 10 am to 1 pm

doubts@cnpd.pt

The initiative taken by the person responsible for the treatment or by the subcontractor to mitigate the damage suffered by the holders - we value the conduct of the defendant who adopted, from the moment of the inspection, the appropriate measures to rectify the detected shortcomings, which are or have already been implemented or under implementation

The degree of responsibility of the person responsible for the treatment or the processor taking into account the technical or organizational measures implemented by them under the terms of articles 25 and 32 - the defendant's responsibility is considered to be high regarding the violation of the restrictions of the levels of access for professionals to the personal data of clients, since it consciously allowed the association of the functional group of "DOCTOR" to those who should only be accredited with the profile of "TECHNICIAN"; As for the lack of procedures to verify the need to maintain the profiles of access for doctors who are no longer at the service of the cannot fail to consider a degree of responsibility

equally high on the part of the defendant, since it was her exclusive responsibility to ensure the control of the need and elimination of these profiles, namely through adequate auditing 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 infraction and mitigate its possible negative effects - which is considered adequate, given, not only, the correction of the detected shortcomings, but also the fulfillment of 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 undue access allowed with the defendant's conduct constitutes a serious interference in their privacy;

How the supervisory authority became aware of the breach, in particular whether the controller or processor notified it, and if so, to what extent they did so - whether the breaches were known

THE

through news from the media 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 previously been imposed on the person responsible for the treatment or the processor in question in relation to the same matter - this criterion not being applied, since there were no any previously determined corrective measures;

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

and

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

the aggravating factor, regarding the offense relating to the violation of Article 32, paragraph 1, items 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 disregard this obligation; the mitigating factor, the fact that the monitoring parameters of the LOGS of access to SClinic information do not depend on the defendant, but rather on the SPMS.

■ Application of the fine

In view of the aforementioned criteria, the CNPD considers it necessary to impose, in this 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 infractions occurred.

As expressed in the deliberation project, the framework of the fine abstractly applicable to the defendant for the foreseen and punishable infractions under the terms of the

combined provisions of Articles 5, paragraph 1 al. c) and article 5, no. 1 al. f) with article 83, no. 5, par. a), of the General Regulation on Data Protection (Regulation 679/2016, of April 27, hereinafter RGPD), punishable, each of them, with a fine of € 0.00 to € 20,000,000.00 or up to 4% of annual turnover, depending on the highest amount, as well as the commission of an infringement, in competition, provided for and punishable under the combined provisions of article 32, paragraph 1, subparagraphs b) and d) and article 83, no. 4, par. a), of the GDPR, with a fine of €0.00 to €10,000,000.00 or up to 2% of annual turnover, whichever amount is higher.

It turns out, however, that after consulting the report and accounts of the defendant, for the year 2017

a result is observed

liquid of

This means that the concrete framework of the fines to be applied is set, in the first case, between €0.00 to €20,000,000.00 and, in the second case, between €0.00 to €10,000,000.00.

Valuing the facts found in the light of the above-mentioned criteria, and considering the fact that the defendant has endeavored to regularize the situation, the CNPD,

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

pursuant to article 58, paragraph 2, par. i) of the RGPD, the imposition of a fine of € 100,000.00 (one hundred thousand euros) on the accused for committing the offense foreseen and punishable under the terms of the combined provisions of articles 32, paragraph 1, subparagraphs b) and d) and article 83, no. 4, par. a), all of the aforementioned regulation.

In addition, under the terms of article 83, paragraph 3 of the RGPD, the fine of € 400,000.00 (four hundred thousand euros).

PrPrêêê§áb°r^9§l^8 i|b 1|o 10

NATIONAL COMMISSION

DATA PROTECTION

VI - Conclusion

r

In view of the above, the CNPD decides:

Apply to the defendant observing the

provided for in paragraph 3 of article 83 of the RGPD, a single fine, in the amount of € 400,000.00 (four hundred thousand euros) due to the violation of the principles of data minimization and integrity and confidentiality, as well as the violation the obligation to apply adequate technical and organizational measures to ensure a level of security appropriate to the risk, namely, a process for regularly testing, evaluating and evaluating the effectiveness of technical and organizational measures to guarantee the security of the processing.

Pursuant to Articles 58, paragraphs 2 and 3 of Decree-Law No. 433/82, of October 27, current wording, inform the defendant that:

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

b) In the event of judicial challenge, the Court may decide at a hearing or, if the defendant and the Public Prosecution Service 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.

Weekdays from 10 am to 1 pm

doubts@cnpd.pt

Process No. 9932/2018 10v

Lisbon, October 09, 2018

\s (íVj

Joao Marques (re

' L í ô

Luis Barroso

r

actor)

Maria Candida Guedes de Oliveira

Pedro Mourao

Filipa Calvao (President)