938-0419

Procedure No.: PS/00132/2019

RESOLUTION OF PUNISHMENT PROCEDURE

In sanctioning procedure PS/00132/2019, instructed by the Spanish Agency for Data Protection, before the entity CLINICAS VIVANTA SL with NIF B82809492, (in hereinafter "the claimed entity"), by virtue of the security breach notified to this Agency, dated 11/20/18, and based on the following:

BACKGROUND

FIRST: On 11/20/18, CLINICAS VIVANTA S.L, notifies this Agency a security breach in which they report that: "Dated 11/15/18, the a PENDRIVE with images of the face of patients for treatments and studies dental. Among the patients whose images were recorded there were minors. There was a person responsible for inserting and removing the memory device, he was also responsible for its custody. When not in use it was kept in a drawer in an office with restricted access".

They have reported the facts to the National Police, (provide a copy of the complaint) and have sent a communication to all employees with the prohibitions on the use of portable devices and the civil responsibility derived from it. They have reviewed the access logs in order to know the last person who used it. They have recovered the images that existed in a computer of the clinic and have installed a image management program used in orthodontics.

They provide a security breach report, dated 11/19/18, which states revealed that: "On the 16th, the person in charge of the PENDRIVE where the images from the camera that were made of the clinic's patients, communicates to the Director of the Center who has disappeared and thinks that someone has taken him.

The device did not have a security key to access, so they consider it a

possible security breach. The data contained in the device was in addition to

the images the name and surname of the patients. The consequences could be

possible disclosure of information.

SECOND: In view of the facts set forth in the documents provided, the

Subdirectorate General for Data Inspection proceeded to carry out actions for its

clarification of the facts, under the investigative powers granted to

the control authorities in art. 57.1 of the RGPD and thus, on 01/28/19, it is directed

informative request to the entity CLINICAS VIVANTA SL., requesting, among others,

information on the causes that have made the incidence possible.

THIRD: On 02/15/19, the entity CLINICAS VIVANTA S.L, provides the

following information: "The PENDRIVE that disappeared has not been located, so

they do not have new information about the reported breach or regarding the

police report. In addition to the measures that have been detailed in the communication of

the security breach, dated 11/24/18 sent to all Clinics by mail

corporate email, the company's Security Policy. They do not have

knowledge of the use by third parties of the data obtained through theft.

Images taken for orthodontic treatment that are performed in the

clinical, therefore, the image taken is not complete, and it is not enough information

to carry out identity theft activities. They have not reported the incident

to those affected, since their orthodontic treatments have not been affected.

They provide a copy of the impact assessment carried out in relation to this treatment

of data "Photographs for dental treatment" in which it is determined that: "It has been

evaluated the probability of impact of 56 threats, being the result of the analysis

of risks of this treatment weighted as ACCEPTABLE; must be implemented

data encryption and personal data dissociation policies and once

Once the measures have been implemented, it will be necessary to review and verify their effectiveness.

FOURTH: On 04/10/19, the Director of the Spanish Agency for the Protection of

Data agreed to initiate sanctioning proceedings against the claimed entity, by virtue of

the powers established in article 58.2 of the RGPD and in articles 47, 64.2 and

68.1 of Organic Law 3/2018, of December 5, on Data Protection

Personal and Guarantee of Digital Rights (LOPDGDD), for the infringement of the

article 32.1 of the RGPD typified in article 83.4.a) of the RGPD and considered serious,

for prescription purposes, in 73.f) of the LOPDGDD.

It is also indicated that, for the purposes provided in art. 64.2 b) of Law 39/2015, of 1

of October, of the Common Administrative Procedure of the Public Administrations,

the sanction that could correspond would be a WARNING, without prejudice to what

that results from the subsequent instruction.

FIFTH: Once the initiation agreement has been notified, the entity CLINICAS VIVANTA SL., through

brief dated 04/29/19, made, in summary, the following allegations:

“(…) CLINICS VIVANTA made the security breach notification. The

information that on the day it was provided was made with the understanding that the

The aim of the regulations with this notification measure is to guarantee the privacy

and the rights of those potentially affected, in order to know the scope that can

to have and be able to carry out the actions that are considered appropriate, and not

as a pretext to open a sanctioning procedure.

However, this action may be contrary to good faith, since, once

there has been proof of all the affected information, which was also

communicated to the AEPD as a result of the request for further information on the security breach, which was answered in a timely manner by this party, the facts would not give rise to the communication of a security breach in the terms established by the AEPD in its informative guide on them, given that the total number of affected does not exceed the number of 20 people, the images that were contained in the pen drive, they did not reflect the totality of the image of the patients, and to date there has been no evidence of a claim/complaint for part of any of the subjects whose images contained the pen drive.

The AEPD in its guide to security breaches, specifically indicated that "in relation to to the possible sanctions that could derive from them, to say that the notification will not directly imply the imposition of a sanction by the AEPD, this would be the result of a lack of due diligence by those responsible and in charge when it supposes the lack of adequate security measures of the treatments and produce a possible damage to the rights and duties of the interested parties".

The entity considers that it has taken sufficient diligence measures, and in At no time has the incidence occurred due to a total lack of safety measures.

security, since the lost pen drive was located in a locked drawer, with access restricted only to a person who had the authorization for its use and handling, and we insist again, there has been no knowledge of damage to the rights and duties of the interested parties who may have been affected by the incident, that there has been no record of any claim, and none of them has been seen affected in the continuity of health care that to date has been been lending

Therefore, CLÍNICAS VIVANTA would be penalized for "excessive diligence", something that seems totally contrary to the spirit of the regulations.

Likewise, regarding the constant indication of the lack of security measures,

that the AEPD marks in its writing, CLINICS VIVANTA, once the scope of the

of the incidence, and this has been notified both in the first communication of 22

November 2018, as in the second dated February 15, 2019, has

An internal response protocol has been established for this type of situation, which includes:

Presentation of a complaint to the Police in order to record the loss of the pen

drive; communication to all users about the obligations in terms of

safety and specifically on the use of memory sticks, which is appropriate

for the correct protection of the data and that has been infringed by the user

that he has lost the information and, for which he was duly sanctioned by

CLINICAS VIVANTA and in addition, measures have been carried out

complementary measures to prevent a contingency of this type from occurring again.

Type.

Therefore, it has been accredited in compliance with the duty of care before the

incidence, during the same (preventive communication of the facts to both the

Police and the AEPD) and after them (adoption of disciplinary measures

against those responsible and reinforcement of the security measures adopted).

As this party has pointed out in this document, to date there has been no

had knowledge or proof of any claim by any of the

affected whose information may have been affected by the incident here

controversial.

The provision that to date has been performing on the subjects

affected, has not been interrupted at any time, nor has it had to be delayed in

case, so there has been no impact on the rights and duties

of these subjects, therefore not producing one of the factors

that in the words of the AEPD itself in its guide to security breaches, they are precise

for the initiation of a sanctioning procedure derived from the notification of a

security breach.

In any case, the total number of those affected by the incident is very small,

exceeding the number of 20 interested subjects, and in any case, the consequences

known to affect your privacy, as we have already indicated, or they do not exist,

or have not been disclosed to this party to date.

The information that has been affected by the incident is about photographs of the

mouths of patients who were undergoing orthodontic procedures, it is

that is, partial images of the patients' mouths that were used with the only

purpose of knowing the evolution of the treatment, so that the use that can be

derive from the images by an unauthorized third party, may not give rise to

consequences on the rights and freedom of the interested parties affected.

SIXTH: On 03/15/19, the testing period began, agreeing:

a).- consider reproduced for evidentiary purposes the documentation provided by the

Technological Studies Unit on the communication of the security breach, the

documents obtained and generated that are part of file E/10485/2018 and

b).- consider reproduced for evidentiary purposes, the allegations to the agreement to initiate the

PS/132/2019, presented by the denounced entity.

SEVENTH: On 05/29/19, the sanctioning resolution proposal is notified

consisting in that by the Director of the Spanish Agency for the Protection of

Data proceed to file this sanctioning procedure as there is no

violation of the provisions of the RGPD.

EIGHTH: Once the resolution proposal has been notified, the entity does not present any type of allegations to the same, in the period granted for this purpose.

In view of everything that has been done, by the Spanish Data Protection Agency

In this proceeding, the following are considered proven facts:

PROVEN FACTS

1º On 11/20/18, CLINICAS VIVANTA S.L, notifies this Agency of a Security breach in which they report that, on the fifteenth of the same month, a pendrive disappeared, from one of his clinics, with images of the treatment oral care of twenty patients.

2º On 02/15/19, the entity indicates that the flash drive has not yet been located. Nope However, they were sent to all the clinics by corporate email, the Company Security Policy. They are also unaware of the use by third parties of the data obtained through theft. They have not reported the incident to those affected, since their orthodontic treatments have not been affected.

3º The entity provides a copy of the impact assessment carried out in relation to this data processing, in which it is determined, among others, that: "The probability of impact of 56 threats, being the result of the risk analysis of this treatment weighted as ACCEPTABLE; Policies should be implemented data encryption and dissociation of personal data and once the measures, it will be necessary to review and verify their effectiveness.

4º In the letter dated 04/29/19, the entity indicates that it has established a protocol internal response to this type of situation, which includes: “the presentation of report to the police. Communication to all users about the obligations in matter of security and specifically on the use of portable memories, which is suitable for the correct protection of the data to avoid that it can return to such a contingency occurs.

5º To date there has been no knowledge or evidence of any by

any of those affected whose information may have been affected by the incident

controversial here.

5/6

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each authority of

control, and as established in art. 47 of the LOPDGDD, the Director of the Agency

Spanish Data Protection is competent to resolve this procedure.

II

Sections 1) and 2), of article 58 of the RGPD, list, respectively, the

investigative and corrective powers that the supervisory authority may provide to the

effect, mentioning in point 1.d), that of: "notifying the person in charge or in charge of the

treatment of alleged infringements of these Regulations" and in 2.i), that of:

"impose an administrative fine under article 83, in addition to or instead of the

measures mentioned in this section, according to the circumstances of each

case.".

The joint assessment of the documentary evidence in the procedure brings to

knowledge of the AEPD a vision of the performance of the claimed entity, which has

reflected in the facts declared proven.

In the present case, the entity has declared the impact assessment, in relation to

the risk in the processing of personal data, as acceptable since the images

taken for orthodontic treatment are not complete, not being information

enough to carry out identity theft activities. It also indicates that

has established an internal response protocol in this type of situation, such as

are, a complaint to the National Police, instructions to employees about the

Prohibitions on the use of portable devices and the civil responsibility derived from

this, review of the records of access to the devices and the installation of a

image management program that will include data encryption and dissociation

personal.

Therefore, from the information provided by the entity to this Agency, both in the

prior inspection as in the allegations at the initiation of the file,

It follows that the possible deficiencies in terms of security measures have been

corrected to avoid a new problem, and, in this way, comply with the provisions of

Article 32.1 of the RGPD, in relation to the processing of data and the measures

technical and organizational measures necessary to guarantee an acceptable level of security.

In view of the aforementioned precepts and others of general application, the Director of the Agency

Spanish Data Protection RESOLVES:

FIRST: FILE this sanctioning procedure against the entity

CLINICAS VIVANTA SL, for an alleged infringement of article 32.1) of the RGPD.

SECOND: NOTIFY this resolution to the entity CLINICAS VIVANTA SL.

In accordance with the provisions of article 50 of the LOPDPGDD, this

Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with art. 48.6 of the

LOPDPGDD, and in accordance with the provisions of article 123 of the LPACAP, the

Interested parties may optionally file an appeal for reconsideration before the

Director of the Spanish Agency for Data Protection within a month from

counting from the day following the notification of this resolution or directly

contentious-administrative appeal before the Contentious-Administrative Chamber of the National Court, in accordance with the provisions of article 25 and section 5 of the fourth additional provision of Law 29/1998, of July 13, regulating the Contentious-administrative jurisdiction, within a period of two months from the day following the notification of this act, as provided in article 46.1 of the aforementioned Law.

Sea Spain Marti

Director of the Spanish Data Protection Agency