Procedure No.: PS/00078/2019

938-0419

RESOLUTION OF PUNISHMENT PROCEDURE

Of the procedure instructed by the Spanish Agency for Data Protection and

in consideration of the following

BACKGROUND

FIRST: Ms. A.A.A. (hereinafter, the claimant) filed on 09/28/2018 with the

Spanish Agency for Data Protection (hereinafter AEPD) a claim in the

stating that Ms. B.B.B., with NIF ***NIF.2 -Santa Fe Physiotherapy Clinic- (in

hereinafter, the claimed one) has sent to an email address that does not

belongs to your medical reports, which contain your personal data.

He adds that the data protection document that the respondent gave him to sign

it only mentioned Organic Law 15/1999, on the Protection of Character Data

Personal, without referring in any case to the provisions of the General Regulations of

Data Protection (EU) 2016/679, which makes you suspect that the documentation

that he signed “does not fully comply with the current norm.”

Accompany the written claim with a copy of the following documents:

-

-

Printout of the email you sent to the Santa Fe Physiotherapy Clinic

on 09/07/2018 which included, as an attachment, the medical report

that they had requested.

Printout of the email that the claimed party sent to a recipient

incorrect.

- Complaint sheet from the General Directorate of Commerce, Consumption and

Economic Cooperation of the Ministry of Labor and Industry of the Board of

Andalusia, completed and signed by the claimant, bearing the stamp of

presentation before the Provincial Delegation of the Consumer Service of

Grenade.

SECOND: In view of the facts set forth, the AEPD, in accordance with the provisions of

Article 9.4 of Royal Decree-Law 5/2018, on urgent measures for adaptation

of Spanish Law to the regulations of the European Union regarding the protection of

data, in the scope of file E/7715/2018, by letter dated

10/22/2018, transferred the claim to the respondent to proceed with its

analysis, inform this Agency, within a month, of the causes that in his opinion

had caused the incident that gave rise to the claim and communicated to the

complainant the measures adopted in this regard.

The documentation is in the file that proves that the claimed received the

10/25/2018 the letter from the AEPD in which the claim was transferred. The

Responded to the information request of the Agency in writing dated

12/13/2018, to which he attached a copy of the letter he sent to the claimant explaining

the origin of the events -which were due to an error when writing your email address-

and that attempts to contact the

owner of the electronic address to which, by mistake, the document was sent

addressed to her and with which her medical report was attached. In that letter addressed to the

claimant the claimed reiterated the apologies that she had already offered when the

The report was delivered personally to the Municipal Police, after

fill out a Consumer Claims form. The defendant accredits

through a Post Office certificate the sending by burofax to the claimant of the document

mentioned.

The AEPD notified the claimant of the actions carried out in writing dated

10/22/2018 which is received on 10/31/2018.

In accordance with the provisions of article 65.5 of the LOPDGDD, on the date

12/21/2018, the AEPD agreed to admit the claim for processing and notified such agreement to the

claimant.

Within the framework of reference file E/00458/2019, in accordance with the provisions

in article 58.1 of the RGPD and 67 of the LOPDGDD, actions of

preliminary investigation aimed at clarifying the facts for which it was requested

additional information to that requested.

The Report of Previous Inspection Actions is transcribed below

E/00458/2019:

<<

1 On September 7, 2018, the complainant sends to the Clinic of

Physiotherapy and Rehabilitation Santa Fe the medical report requested in visit

face-to-face to determine the appropriate treatment.

1. On September 14, 2018, the clinic sent to an email address

erroneous treatment corresponding to the interested party.

2. In the briefs received, it is observed that the difference between the address of

mail of the interested party and the wrong mail address, there is a variation in

one letter. Instead of sending the information to the address ***EMAIL.1, it was sent to

***EMAIL.2

3. From this wrong address, the email address was not received.

from the clinic error report by the destination server, which wants

say that it is a valid email address and that the report with the treatment

has been delivered to this email address.

4. On January 28, 2019, this Agency received the number of

registration ***REGISTRATION.1, written from the Physiotherapy Clinic and

Rehabilitation Santa Fe, where it is stated that the email address of the

interested, word was collected. They state in this writing that they have tried

contact the person to whom this email address corresponds

wrong mail without success. They have also searched social networks with the

name of “Rose Ish” finding a reference to this name in

Facebook but without identification, biography, photos, or friends.

They also attach the authorization for the processing of personal data

signed by the complainant on September 7, 2018 collecting the

application of the regulations of Law 15/1999. They also attach forms

updated to Regulation (EU) 679/2016. >>

THIRD: On March 5, 2019, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the one claimed by the

alleged infringement of articles 13 and 32 of Regulation (EU) 2016/679, of the

European Parliament and of the Council, of 04/27/2016, regarding the Protection of

Natural Persons with regard to the Processing of Personal Data and the Free

Circulation of these Data (General Data Protection Regulation, hereinafter

GDPR)

FOURTH: The agreement to initiate the sanctioning procedure PS/78/2019 was

notified to the respondent on 03/11/2019.

The respondent did not make allegations to the agreement to initiate the file

sanctioning There is no news in this body of the entry of any writing of

the claimed one through which it complies with the process of allegations that it grants

the law.

Article 64.2.f) of Law 39/2015, of October 1, on the Procedure

Common Administrative of Public Administrations (LPACAP) indicates that, in

If you do not make allegations within the stipulated period on the content of the agreement of

initiation, it may be considered a resolution proposal when it contains a

precise statement about the imputed responsibility.

Taking into account that the term established in the LPACAP to make allegations to the

agreement to start the sanctioning file was far exceeded without the

claimed had evacuated the procedure, and, since said agreement contained -as

as required by article 64.2.f) of the LPACAP- “a precise statement about the

imputed responsibility”, we must conclude that, in the case at hand, the

The aforementioned initial agreement is considered a resolution proposal, so that the

The instructor of the file raises it without further formalities to the competent body for

resolve (former article 88.7 LPACAP).

In this procedure the following have been accredited,

FACTS

1st. The claimant, Ms. A.A.A., with NIF ***NIF.1, and owner of the electronic address

“***EMAIL.1” denounces that the Santa Fe Physiotherapy Clinic -commercial name under

the one who operates the claimed company as a self-employed entrepreneur- sent a report

doctor with your personal data to an electronic address that does not belong to you.

He adds that the documentation that he signed in that company, relating to the protection of

data, was not adapted to current regulations because it still mentioned the Law

Organic Law 15/1999 on the Protection of Personal Data.

2nd: Copies of the following emails are in the file

1. Sent on 09/07/2018 at 19:32 from ***EMAIL.1 to

***EMAIL.3 with the following text:

“(…) As agreed, I send medical report….”.

Attached to this email is a pdf document called

“***DOCUMENT.1f”.

2. Sent on 09/14/2018 at 8:47 a.m. from the address

***EMAIL.3 to the address ***EMAIL.2. As "Subject" of the email

figure "report". The mail is signed by the claimed

(identified by her name and two surnames) and immediately

below the indication "Physiotherapist" and the number of collegiate.

3º: The respondent has recognized that, due to "an error", she sent the medical report of the

claimant to an email address that was not the one she had provided. The

error consisted -according to their explanations- in writing as electronic address of

destination “NAME.2” instead of “NAME.1”, which was the correct address and the one that

acknowledges that the claimant had provided

4th: The respondent informed the AEPD in her brief of 02/13/2019, in which she responded

to the informative requirement of the Agency in E/7715/2018, that “Since the detection

of the error the decision has been made to send the medical reports of the patients

who request it by electronic means without including their personal identification data".

5º: The respondent, in her brief of 01/28/2019, within the framework of E/4355/2019, acknowledges

that the information provided to the claimant when collecting her personal data is not

was updated to current regulations and still referred to the Organic Law

15/1999. Provide a copy of the document, which appears signed by the claimant on

09/07/2018 in which the possibility of exercising access rights is reported,

rectification, cancellation and opposition and the identity of the person in charge.

6º: The respondent contributed with her letter of 01/28/2019 in response to the request

of the data inspection, a copy of the informative document that, as

responsible for the treatment is currently provided to the people of the

that collects personal data.

The document is adapted to EU Regulation 2016/679 and it provides

information about the identity of the data controller; of the purpose of

treatment; of the legal basis of the treatment; of the consequences of not facilitating

your personal information; of the possibility of communicating them to the health personnel who

works for the person in charge or to Public Administrations with competence in the

matter; of the term for its deletion; of the possibility of exercising the rights of

access, rectification, suspension, limitation of treatment or opposition to treatment and

to file a claim with the supervisory authority.

In addition, the respondent provided with her brief of 01/28/2019, a form to

that patients can exercise before it the rights recognized in articles

15 to 22 of the GDPR.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of Regulation 2016/679 (EU) of

data protection (hereinafter RGPD) recognizes each control authority, and

according to the provisions of articles 47 and 48.1 of Organic Law 3/2018, of 5

December, Data Protection and Guarantees of digital rights (LOPDGDD),

The Director of the Spanish Data Protection Agency is competent to

resolve this procedure.

Article 5 of the RGPD, “Principles related to treatment”, mentions among them

those of “transparency” and “integrity and confidentiality”. The precept establishes:

II

“Personal data will be:

a) processed in a lawful, loyal and transparent manner in relation to the interested party

(<<legality, loyalty and transparency>>)

(…)

f) processed in such a way as to guarantee adequate security of the data

including protection against unauthorized or unlawful processing and against

its loss, destruction or accidental damage, through the application of technical measures

or appropriate organizational (<<integrity and confidentiality>>)”

Article 13 of the RGPD, under the heading “Information to be provided

when the personal data is obtained from the interested party”, it says:

"1. When personal data relating to him is obtained from an interested party, the

responsible for the treatment, at the time these are obtained, will provide

all the information indicated below:

a) the identity and contact details of the person in charge and, where appropriate, of their

representative;

legal treatment;

b) the contact details of the data protection delegate, if applicable;

c) the purposes of the treatment to which the personal data is destined and the basis

Their case;

d) when the treatment is based on article 6, paragraph 1, letter f), the

legitimate interests of the person in charge or of a third party;

e) the recipients or the categories of recipients of the personal data, in

f) where appropriate, the intention of the controller to transfer personal data to a

third country or international organization and the existence or absence of a decision to

adequacy of the Commission, or, in the case of transfers indicated in the

Articles 46 or 47 or Article 49, paragraph 1, second paragraph, reference to the

adequate or appropriate warranties and the means to obtain a copy of these or

to the fact that they have been borrowed.

2. In addition to the information mentioned in section 1, the person responsible for the

treatment will facilitate the interested party, at the moment in which the data is obtained

personal, the following information necessary to guarantee data processing

fair and transparent

a) the period during which the personal data will be kept or, when it is not

possible, the criteria used to determine this period;

b) the existence of the right to request from the data controller access to

the personal data related to the interested party, and its rectification or deletion, or the

limitation of its treatment, or to oppose the treatment, as well as the right to

data portability;

c) when the treatment is based on article 6, paragraph 1, letter a), or the

Article 9, paragraph 2, letter a), the existence of the right to withdraw consent in

any time, without affecting the legality of the treatment based on the

consent prior to its withdrawal;

d) the right to file a claim with a supervisory authority;

e) if the communication of personal data is a legal or contractual requirement, or

a necessary requirement to sign a contract, and if the interested party is obliged to

provide personal data and is informed of the possible consequences of

not provide such data;

f) the existence of automated decisions, including profiling, to

referred to in article 22, sections 1 and 4, and, at least in such cases, information

about applied logic, as well as the importance and consequences

provisions of said treatment for the interested party.

3. When the person in charge of the treatment projects the subsequent treatment of

personal data for a purpose other than that for which it was collected,

will provide the interested party, prior to said further treatment, information

for that other purpose and any additional information relevant to the meaning of paragraph 2.

4. The provisions of sections 1, 2 and 3 shall not apply when and in the

to the extent that the interested party already has the information.>>

The violation of the duty to inform the interested party from whom data is collected

in the terms required by article 13 of the RGPD is typified

in article 83.5. of the RGPD, a precept that establishes:

"Infringements of the following provisions will be sanctioned in accordance

with section 2, with administrative fines of a maximum of EUR 20,000,000 or,

in the case of a company, an amount equivalent to a maximum of 4% of the

global total annual turnover of the previous financial year, opting for

the largest amount:

(…)

the rights of the interested parties under articles 12 to 22;"

The LOPDGDD, for prescription purposes, qualifies in its article 72.1.h as

very serious infraction the omission of the duty to inform the affected party about the

processing of your personal data in accordance with the provisions of articles 13 and 14

of EU Regulation 2016/679.

In turn, article 32 of the RGPD, regarding "Data Security", states:

"1. Taking into account the state of the art, the application costs, and the

nature, scope, context and purposes of the treatment, as well as risks of

variable probability and severity for the rights and freedoms of individuals

physical, the person in charge and the person in charge of the treatment will apply technical measures and

appropriate organizational measures to guarantee a level of security appropriate to the risk,

which in your case includes, among others:

a) pseudonymization and encryption of personal data;

b) the ability to ensure the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

c) the ability to restore the availability and access to personal data

quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and assessment of the effectiveness of

the technical and organizational measures to guarantee the security of the treatment.

2. When evaluating the adequacy of the security level, particular account shall be taken of

takes into account the risks presented by the processing of data, in particular as

consequence of the accidental or unlawful destruction, loss or alteration of data

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data.

3. Adherence to an approved code of conduct under article 40 or to a

certification mechanism approved under article 42 may serve as an element

to demonstrate compliance with the requirements established in section 1 of the

present article.

4. The person in charge and the person in charge of the treatment will take measures to

guarantee that any person acting under the authority of the controller or the

manager and has access to personal data can only process said data

following the instructions of the person in charge, unless it is obliged to do so by virtue of the

Law of the Union or of the Member States.>>

The violation of the obligation imposed by article 32 of the RGPD is

It is typified in article 83.4 of the RGPD, a precept that establishes:

“The infractions of the following dispositions will be sanctioned in accordance with

section 2, with administrative fines of a maximum of EUR 10,000,000 or,

in the case of a company, an amount equivalent to a maximum of 2% of the

global total annual turnover of the previous financial year, opting for

the largest amount:

a) The obligations of the person in charge and the person in charge pursuant to articles …

25 to 39…”

The LOPDGDD, for prescription purposes, qualifies in its article 73 f) as

serious infraction the lack of adoption of those technical and organizational measures that

are applicable to guarantee a level of security appropriate to the risk of the

treatment, in the terms required by article 32.1 of the Regulation (EU)

2016/679.

It is attributed to the claimed in this sanctioning file the infraction of the

articles 13 and 32 of the RGPD. The behaviors in which this infraction is specified

consisted, on the one hand, in not providing the claimant at the time of collecting her

personal data the information referred to in article 13 of the RGPD, and on the other,

III

in having omitted the security measures that it was obliged to adopt, under

of article 32 of the RGPD, when he sent by email a medical report of

the claimant with health data to an address that turned out to be wrong.

a.- Regarding the infringement of article 13 RGPD, the defendant has recognized

that the information provided to the claimant did not comply with current regulations.

It has provided a copy of the informative document that the claimant signed in September

of 2018 (RGPD in force since 05/25/2018) whose content complied with the LOPD

and not to Regulation 2016/679.

Thus, the file fully accredits the violation by the

claimed, in relation to the processing of the personal data of the claimant,

of article 13 of the RGPD.

Now, it should be underlined that the respondent has contributed to this Agency in the same date the new informative document that provides third parties of whom collect personal data. As detailed in Proven Fact 6, the document information complies with the requirements of article 13 of the RGPD.

b.-Regarding the infringement of article 32 of the RGPD of which holds the defendant responsible has been fully accredited in accordance with the documents that are in the file and what was stated by her in her response to the informative requests that were made.

In the second Proven Fact, the email that the claimed sent on 09/14/2018, with which the medical report that the claimant had transferred days before, on 09/07/2018, also as a document exhibit. It is verified in this email that the e-mail address of the claimant is "***EMAIL.1" while the claimed one sent hers to a different address "***EMAIL.2

The documents that are in the file and the declarations of the claimed evidence that it had not adopted any measure to guarantee the integrity of the personal data it processes, in particular on the occasion of its communication through electronic means.

The defendant, in response to the request made by the AEPD before the opening of the agreement to start the file to report on the measures adopted to prevent similar events from occurring in the future, reported in written on 02/13/2019 that "Since the detection of the error, the decision has been made to send the medical reports of patients who request it by electronic means without including your personal identification data".

With regard to the measure that it claims to have adopted, we must point out that

it seems that such a decision means a real guarantee of the integrity of the data
treatment object. On the one hand, because, although the email does not identify the
recipient by name, surname and NIF, on many occasions the addresses of
mail incorporate one or more of these data. On the other, because, in addition to
the documents of the medical report usually include these data, the concept of data

personal is not limited to name, surnames and NIF. Article 4.1) of the RGPD
understands personal data as “all information about an identified natural person or
identifiable (“the interested party”); An identifiable natural person is considered to be any person
whose identity can be determined, directly or indirectly, in particular by
an identifier, such as a name, an identification number,
location, an online identifier or one or more elements of the identity
physical, physiological, genetic, psychic, economic, cultural or social of said person”.
Therefore, in relation to the infringement of article 32 of the RGPD, typified in the
article 83.4 of that rule, for which the defendant is responsible, it has not
accredited to have adopted any measure with virtuality to guarantee the
compliance with the obligations imposed by the violated precept.

Article 58 of the RGPD, “Powers of Attorney”, says:

IV

“2 Each supervisory authority shall have all of the following powers
corrections listed below:

(…)

b) sanction any person responsible or in charge of the treatment with a warning

when the treatment operations have violated the provisions of this

Regulation;

(...)

d) order the person in charge or in charge of the treatment that the operations of

treatment comply with the provisions of this Regulation, where appropriate,

in a certain way and within a specified period.

(…)

i) impose an administrative fine under Article 83, in addition to or instead of

of the measures mentioned in this section, depending on the circumstances of the

particular case

(…)"

Despite the fact that articles 83.5 and 83.4 RGPD provide for a sanction of a fine

administrative, respectively, for infractions of articles 13 and 32 of the

RGPD for which the claimed party is responsible, article 58.2 of the RGPD

contemplates the possibility of sanctioning infractions of this Regulation with

"warning".

On the origin of opting for the sanction of warning and not for the fine

administrative provision provided for in articles 83.4 and 5 RGPD, it is worth mentioning, as

element that allows an authentic interpretation of the rule, Recital 148

of Regulation 2016/679 that contains this reflection:

"In the event of a minor offence, or if the fine likely to be imposed

would constitute a disproportionate burden for a natural person, rather than

sanction by means of a fine, a warning may be imposed. must however

Special attention should be paid to the nature, seriousness and duration of the infringement, its

intentional nature, to the measures taken to alleviate the damages suffered,

the degree of liability or any relevant prior violation, the manner in which

that the control authority has been aware of the infraction, compliance

of measures ordered against the person responsible or in charge, adherence to codes of

conduct and any other aggravating or mitigating circumstance" (Emphasis added).

the AEPD)

In order to determine the sanction that is appropriate to impose for the infraction

of articles 13 and 32 of the RGPD for which the claimed party is responsible,

take into consideration factors as relevant as the character of the entrepreneur

autonomous of the natural person responsible for the treatment; the collaboration that has

provided to this Agency, since it responded promptly to the two requirements that

they were made to him; the measures it adopted in the face of the irregular situation caused -we

we refer to the sending to the claimant by burofax dated 11/26/2018 of a letter

in which he recognized the mistake made and apologized, the adequacy of his policy

of data protection to the provisions of article 13 of the RGPD, current regulation

since 05/25/2018 and, therefore, in force when the claimant went to the

establishment of the claimed and provided their personal data-; the rectification

made in their files of the inaccurate data -the claimant's email address-; the

actions you have taken to try to locate the owner of the address

to which you mistakenly sent the claimant's medical report along with your

identification data -which is exponent of your statement that the search has been

specified only in a reference found

on Facebook to

"***REFERENCE.1" without profile, or history, or contact, or the decision that, it says, has adopted from the detection of these facts of not including personal data when patients request the submission of their medical records by electronic means, leads to the conclusion that the sanction to be imposed for infractions of the RGPD whose responsibility is attributed to the claimed, be it the warning and not the fine provided for in articles 83.4 and 83.5 RGPD, as it is more in accordance with the spirit of the GDPR in light of Recital 148.

Additionally, under the provisions of article 58.2 of the RGPD that recognizes the control authorities various corrective powers, and in particular of the section d) of the provision, it is deemed appropriate to order the respondent to adopt the technical and organizational measures that are appropriate to ensure a level of security appropriate to the risk involved in the processing of data carried out in accordance with in accordance with article 32 of the RGPD. The adoption of these measures must accredited before this Agency within a month from the date on which the resolution in which they agree is executive.

Regarding this issue, the Agency reiterates that, as explained in the agreement beginning of the file, a type of measure adopted in similar cases that has shown to have consistency to meet the intended purpose is to assign the patient a key or password that only he knows. That key or password is sent to the patient by means other than email, and must be entered the patient to read the messages received via email.

It is also recalled that, if necessary, it is up to the person in charge of the treatment the burden of demonstrating the virtuality of the measures adopted for the fulfillment of the aims pursued and which must be taken into account -because it seems something else can be inferred from the content of the response to the informative request of this

Agency- that the condition of personal data is not predicated solely on the NIF, the

name and surnames. We refer on this particular to the definition of data

personal offered by article 4. 1 of the RGPD.

In relation to the corrective measures of article 58.2 RGPD that is agreed

impose on the defendant in the sanctioning procedure that concerns us, must

It should be remembered that Regulation (EU) 2016/679 sanctions "Failure to comply with the

resolutions of the control authority in accordance with article 58, section 2" with a fine

administration of a maximum of 20,000,000 euros or, in the case of a company,

of an amount equivalent to a maximum of 4% of the total annual turnover

of the previous financial year, opting for the highest amount (article 83.6

GDPR)

Therefore, in accordance with the applicable legislation, the Director of the Agency

Spanish Data Protection RESOLVES:

FIRST: IMPOSE B.B.B. (Santa Fe Physiotherapy Clinic), with NIF ***NIF.2,

for an infringement of article 13 of the RGPD, typified in article 83.5 of the RGPD,

a penalty of warning provided for in article 58.2.b) of the Regulation (EU)

2016/679.

/

SECOND: IMPOSE B.B.B. (Santa Fe Physiotherapy Clinic), with NIF ***NIF.2,

for an infringement of article 32 of the RGPD, typified in article 83.4 of the RGPD,

a penalty of warning provided for in article 58.2.b) of the Regulation (EU)

2016/679.

In accordance with article 58.2.d) of the RGPD, order B.B.B. (Clínica de Fisioterapia Santa Fe), with NIF ***NIF.2, which adopts the technical measures and organizational measures that are necessary to guarantee a level of security adequate to the risk involved in the data processing carried out according to article 32 of the RGPD.

The adoption of these measures must be accredited before this Agency within the term of one month computed from the date on which the resolution becomes executive

THIRD: NOTIFY this resolution to the respondent.

FOURTH: Warn the sanctioned person that she must comply with the sanction imposed once that this resolution is enforceable, in accordance with the provisions of art. 98.1.b) of Law 39/2015, of October 1, of the Common Administrative Procedure of Public Administrations (hereinafter LPACAP)

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 article 48.6 of the LOPDGDD, and in accordance with the provisions of article 123 of the LPCAP, 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

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es