 File No.: PS/00348/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: D.A.A.A. (hereinafter the claimant) on 06/24/2020 filed

claim before the Spanish Data Protection Agency. The claim is

directs against the COMMUNITY OF OWNERS B.B.B., with NIF ***NIF.1 (in

forward the claimed). The grounds on which the claim is based are as follows:

community of owners to which it belongs has made available to the neighbors

that make up a space in the portal https://konvoko.com where they are stored

community documents including the minutes of the owners' meetings; East

portal has a mobile application for access from smartphones to

documents made available to the community in addition to being able to access via

Web.

According to the complainant, once the application is downloaded, it can be freely accessed and

without any type of password or restriction to the records of said community, being able to

view documents in which the personal data of the user would be accessible

interested and provides links that lead to community documents without

no restriction:

It also indicates that the neighbors had not been informed of the existence of a file

registration of treatment activities by the community.

Likewise, it states that the viewing of the cameras of the security system has been carried out.

video surveillance by unauthorized person. On the other hand, he adds that there is no

any document approved by the board of owners where the person is picked up

authorized to access the cameras.

The claimant provides the Certificate of Presence in which the notary attests that the

access various documents relating to the community of owners claimed to

through the mobile application without any restriction, being among these, minutes

of meetings of owners where they are reflected, among other matters, personal data and

defaulting situations of the owners. Attached to this notarial deed is a printout of

a minute of a meeting of owners obtained without any restriction.

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5

December, of Protection of Personal Data and guarantee of digital rights (in

hereinafter LOPDGDD), with reference number E/05334/2020, transfer of di-

this claim to the claimant on 07/31/2020, so that it could proceed with its analysis and information.

report to this Agency within a month, of the actions carried out in order to

comply with the requirements set forth in the data protection regulations. was reiterated

the request on 08/13/2020.

THIRD: On 12/16/2020, the Director of the AEPD agrees to the admission to

limit of the claim.

FOURTH: In view of the facts denounced in the claim and the documents

data provided by the claimant, the Subdirectorate General for Data Inspection pro-

yielded to carry out preliminary investigation actions for the clarification

of the facts in question, by virtue of the powers of investigation granted to the

control authorities in article 58.1 of Regulation (EU) 2016/679 (Regulation

General Data Protection, hereinafter RGPD), and in accordance with the provisions

ed in Title VII, Chapter I, Second Section, of Organic Law 3/2018, of 5

December, of Protection of Personal Data and guarantee of digital rights (in

hereinafter LOPDGDD).

Regarding the publication of data on the KONVOKO TECHNOLOGY platform,

SL (hereinafter Konvoko):

Regarding the portal https://konvoko.com where various documents are stored

of the community, it is verified that, when installing the application indicated in the claim,

mation, you can no longer access the documents of the community of owners

for the simple fact of performing a search with the term (...) as stated in the

notarial act provided by the claimant. It is concluded, therefore, that this aspect has

been remedied.

However, the acting inspector verifies, on 02/03/2020, that despite what

pointed out by Konvoko in the reply to the transfer of the claim on security

information published on this platform, it is still possible to access via

web to the documents indicated in the claim, among which are records with

personal data and situations of non-payment, of public access and without restriction.

Requested information on these events from the company Konvoko, dated

02/17/2021, this Agency receives a response to the request stating that

through the possibility offered by the system of "sharing" a document, it was created

a free access link bypassing the established measures, generating

a security problem that they had not detected. They add that as soon as they received

the requirement of this Agency dated 02/04/2021 proceeded to correct

this problem being solved. It is verified that it is no longer possible to access the

documents indicated in the claim.

Likewise, they present to this Agency an Impact Assessment report on this transaction.

concluding that it can be carried out without significant risks, since none

None of the detected threats has a "high" or "very high" inherent risk.

Regarding the visualization of the images captured by the video surveillance system

Inc:

On the incorrect use of the images recorded by the video surveillance system

community, the claimant does not provide any evidence, but assumptions

about an illicit use of the system based on the statements made by the president

representative of the community in a neighborhood meeting on certain behavior of the

clamoring that they could well have been observed in any other way. In no mo-

moment is cited in these minutes, that this behavior has been observed through the

visualization of images recorded by the video surveillance system or that exist

these images.

However, a request was made to the president of the community of owners

Regarding the statement of the claimant that it is not included in any document

the person authorized to view the images, dated 04/24/2021,

receives in this Agency a written reply stating that the video system

surveillance was approved in various meetings of owners as recorded in the minutes

with dates of March 2012, where the motivation for the installation is collected, and July

2012, where the installation of video surveillance cameras was unanimously approved.

lancia in section 6.2.e. They add that there is a tacit agreement that it be the boards

These directives that are occupying the representation of the community of owners

who exercises the due responsibilities regarding the visualization of the cameras

of video surveillance. Recording equipment and display monitor are located

in the telecommunications room inside a locked metal cabinet,

this being guarded by the board. They point out that the images are not displayed by

no third party.

And they attach, among others, the following relevant documents:

- Minutes dated 03/15/2012 and 07/12/2012

- Photographs of the informative posters of the video-monitored area where the location is indicated.

where to exercise the rights of the interested party.

- Photographic report of camera location and viewing scope. Among

them, photograph of the camera located in the telecommunications room in which

Find the cabinet containing the recording equipment and the viewing monitor.

- Screenshot of the recording management application where it can be seen

They have a life cycle of one month.

FIFTH: On 08/18/2021, the Director of the Spanish Agency for the Protection of

Data agreed to initiate a sanctioning procedure against the defendant, for the alleged infraction

tion of articles 5.1.f) and 32.1 of the RGPD, typified in articles 83.5.a) and

83.4.a) of the aforementioned regulation.

SIXTH: Having notified the aforementioned initiation agreement, on 09/20/2021 the respondent presented

brief of allegations in which, in summary, it stated the following: its disagreement

with the opening of the agreement to initiate the sanctioning procedure considering

do which is null and void; that documentation has not been transferred to

in order to exercise their right to defense and put forward the arguments and evidence they could

counteract the statements made by the complainant, leaving the complaining party

stay in a defenseless situation; that the Konvoco company is responsible for the

processing of the user's personal data; that in any way can be done

liable to the respondent for having to make decisions aimed at implementing

effectively the appropriate technical and organizational measures to guarantee a ni-

level of security appropriate to the risk; which is to the Konvoco company that you have to

direct the procedure for being responsible for the facts.

SEVENTH: On 09/28/2021, the opening of a practice period of

tests, remembering the following:

Consider reproduced for evidentiary purposes the claim filed by the claimant-

te and its documentation, the documents obtained and generated by the Services of

Inspection that are part of file E/10201/2020.

Consider reproduced for evidentiary purposes, the allegations to the initial agreement presented

ted by the claimed party and the documentation that accompanies them.

EIGHTH: On 01/24/2022 the requested Resolution Proposal was notified in the

sense that the Director of the AEPD sanctioned the defendant for infraction

of articles 5.1.f) and 32.1 of the RGPD, typified in articles 83.5.a) and 83.4.a) of the

GDPR, with warning.

After the period established by the claimant, at the time of this Resolution,

He had not submitted any brief of allegation.

NINTH: Of the actions carried out, the following have been accredited

PROVEN FACTS

FIRST. On 06/24/2020 it has entry into the Spanish Data Protection Agency.

written documents of the claimant stating that the community of owners to which he per-

has made available to the neighbors who form it a space in the portal

https://konvoko.com where community documents are stored including

minutes of the meetings of owners; This portal has a mobile application for

access from smartphones to community documents as well as being able to

access via web; The claimant points out that once the application has been downloaded,

access freely and without any type of password or restriction to the minutes of di-

cha community being able to visualize documents in which the

personal data of the interested party and provides links that lead to documents of the

community without any restriction:

It also indicates that the neighbors had not been informed of the existence of a file

registration of treatment activities by the community.

SECOND. Proof provided Diligence of the notary of Las Palmas dated

05/08/2020 in which it is stated, among others, that "The same day of the request, it is

that is to say, on the seven eighth of May of two thousand and nineteen, being twelve hours forty and

five minutes, and with the presence of the applicant in my office on the street ***DIREC-

CIÒN.1, I download the free application “KONKOVO” from my mobile phone.

Once downloaded, I write the word (...) in the search engine and I get several files

in pdf format.

I access the first one, which I print and incorporate into this matrix.

I certify that he has not asked me at any time for passwords or keys to access

der, that is to say, that access is completely open and free”.

THIRD. A copy of the Minutes of the Ordinary Meeting is included in the Diligence

of the Community of owners held on 04/25/2019, which includes data on the

personal character of owners of the community.

FOURTH. A copy of the Minutes of the Ordinary Meeting of the Community of

owners held on 03/14/2016 in which point 9 indicates that "It is reported that the

President of the Community hires in the month of October 2015, for an amount

annual €96 igic included, the Konvoco mobile application…”.; communication in-

posted on the Community Notice Board informing that access to the

neighborhood information will be made through the Konvoco application and through

password, as well as the links:

***URL.1

***URL.2

***URL.3

***URL.4

that lead us to community documents, minutes, agreements and documents of the

Community containing personal data without restriction.

FIFTH. Konvoko in writing of 08/20/2020 has stated that "We believe that

there is no incident that motivates this claim since to access the information

mation of any community of owners that publishes or any other entity of

private profile in Konvoko previously you have to know the password provided and be

validated the request by the person in charge of the community...

We do not know what the channel of communication between the Community and the neighbors has been.

us to send you said password since the current meeting tells us

who have been in charge of it for a short time and it was the old board who registered the

10-13-2015 and launched the app with the neighbors…”

SIXTH. The Inspector's Diligence is recorded stating "... that on February 3, 2021

impression of the pages of the website https://www.konvoko.com of the do-

Claimed Documents:

***URL.1

***URL.2

corresponding to two minutes of the owners' meeting in which personal data is revealed

personal and non-payment situations of the owners".

The acting inspector in his Report has indicated that: "However, the acting inspector

tuante verifies, dated 02/03/2021 despite what was indicated by KONVOKO in the

response to the transfer of the claim on the security of public information

each on this platform, which can still be accessed via the web to the documents

indicated in the claim, among which are records with personal data and

situations of non-payment, public access and without restriction".

SEVENTH. Konvoko in writing of 02/17/2021 states that "The same night of the game-

You see February 4, date of receipt of the request in which the AEPD reported

of the incident, access through shared links was resolved and blocked.

two by users with access to senders in private, although only for devices that

They did NOT have the Konvoko app installed.

- The next day, February 5, access was also blocked for the devices

sites that DO have the app installed.

- On Monday the 8th it was detected that, although access to the texts was already restricted, all-

via it was possible to access an attached pdf, leaving this resolved and inaccessible the same

on the 8th of February".

EIGHTH. The acting inspector in Diligence of 03/09/2021 has indicated that “in this date printout of the results is obtained by directing the browser to the links indicated fallen on the claim. It is verified that the documentation of the community of owners showing as a result the main page of the platform-form KONVOKO”. Concluding in its Report that “therefore, this aspect has been do remedied”.

FOUNDATIONS OF LAW

Yo

In accordance with the powers that article 58.2 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter RGPD), grants each autho-authority of control and according to what is established in articles 47, 48.1, 64.2 and 68.1 of the Law Organic 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (hereinafter, LOPDGDD), is competent to initiate and resolve this procedure the Director of the Spanish Data Protection Agency.

Likewise, article 63.2 of the LOPDGDD determines that: “The procedures Data processed by the Spanish Agency for Data Protection will be governed by the provisions established in Regulation (EU) 2016/679, in this organic law, by the provisions regulatory provisions issued in its development and, as long as they do not contradict them, with subsidiary character, by the general rules on administrative procedures you.".

II

Prior to examining the merits of the matter, it is appropriate analyze the exception alleged by the respondent that, if successful, would invalidate the substantive or material considerations.

The respondent alleges that the procedure is null and void by virtue of

article 47.1 a) and g) of Law 39/2015 by not transferring the documentation

part of the file, especially the notarial certificate "Record of Presence of the

Notary", in order to exercise their right to defense and put forward the arguments and evidence

that could counteract the statements made by the claimant, leaving him in

defenseless situation.

It should be noted that in accordance with article 67 of the LOPDGD, before

of the adoption of the agreement to initiate the procedure, and once the application has been admitted for processing.

claim, if any, the Spanish Agency for Data Protection may carry out

carry out preliminary investigation actions in order to achieve a better determination of the

the facts and circumstances that justify the processing of the procedure. And that

both the claim filed by the claimant and its documentation, the

documents obtained and generated by the Inspection Services that are part

of file E/10201/2020 have been incorporated into it through the practice of

the proof.

Article 67 of the LOPDGDD, Previous investigation actions, establishes

that:

"1. Before the adoption of the agreement to initiate the procedure, and once

Once the claim is admitted for processing, if any, the Spanish Agency for the Protection of

Data may carry out preliminary investigation actions in order to achieve a

better determination of the facts and circumstances that justify the processing of the

process.

The Spanish Agency for Data Protection will act in any case when it is

requires the investigation of treatments that involve massive data traffic

personal.

2. The preliminary investigation actions will be subject to the provisions of the

Section 2 of Chapter I of Title VII of this organic law and may not have a

duration of more than twelve months from the date of the admission agreement to

procedure or the date of the agreement by which its initiation is decided when the Agency

Spanish Data Protection Agency acts on its own initiative or as a consequence of

the communication that would have been sent by the supervisory authority of another State

member of the European Union, in accordance with article 64.3 of this organic law".

Therefore, the infraction imputed to the defendant in this

sanctioning procedure has not been carried out based on mere suspicions or indications,

but because of the evidence obtained that proves the claimed facts.

However, the respondent is informed that Law 39/2015, in its Title

IV, Of the provisions on the common administrative procedure, Chapter I,

Procedural guarantees, in its article 53.1.a) states that:

"1. In addition to the rest of the rights provided for in this Law, those interested in a

administrative procedure have the following rights:

a) To know, at any time, the status of the processing of the

procedures in which they have the status of interested parties; the sense of

corresponding administrative silence, in case the Administration does not

dictate or notify an express resolution within the term; the competent body for

instruction, if any, and resolution; and the procedural acts dictated. Likewise,

They will also have the right to access and obtain a copy of the documents

contained in the aforementioned procedures.

(...).

Article 58 of the RGPD, Powers, states:

III

"two. Each supervisory authority will have all of the following powers

corrections listed below:

b) send a warning to any person responsible or in charge of the treatment when the

treatment operations have violated the provisions of this Regulation;

(…)

(…)”

In the present case, the exposed facts consisting of the fact that the community

of owners to which the claimed person belongs has made available to the neighbors

a platform for access from smartphones to community documents

ity, although access is free and without any type of password to them being able-

the personal data of the interested party will be displayed, constituting an infringement of the

data protection requirement, specifically the principle of confidentiality of data

themselves.

Article 5 of the RGPD establishes the principles that must govern the treatment

of personal data and mentions among them that of “integrity and confidentiality”.

The cited article states that:

"1. The personal data will be:

f) processed in such a way as to ensure 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").

(…)

(…)

IV

It should be noted that for the purpose of the data processing carried out by the

communities of owners in its management is to ensure compliance by the

owners of the obligations imposed by the LPH, as well as guarantee the

adequate exercise of the rights that correspond to the community members and the

third parties in the community.

The condition of data controller falls on the community of

owners.

The documentation in the file shows that the claimed,

violated article 5 of the RGPD, principles related to treatment, by enabling the

access via mobile application to community documents without restriction

some, among which are records with personal data and non-payment situations.

The claimed party considers that it was the claimant himself who has brought about

that your data reach third parties without authorization.

However, such an argument cannot be admitted and bears little resemblance to what

indicated in the fifth proven fact where the Diligence of the notary is extracted

of Las Palmas, dated 05/08/2020, in which it is stated that “On the same day of the

requirement, that is to say, on May 7, 2019, twelve o'clock being

hours forty-five minutes, and with the presence of the petitioner in my office in

the street ***ADDRESS.1, I download the free application from my mobile phone

“KONKOVO”.

Once downloaded, I write the word (...) in the search engine and I get several

files in PDF format.

I access the first one, which I print and incorporate into this matrix.

I certify that he has not asked me at any time for passwords or keys to

access, that is to say, that access is completely open and free".

In other words, there was the possibility that the personal data of which they are

holders the owners were known by third parties outside the

Community, through unhindered access to them as it is not necessary

password or security key, which is a violation of the duty of

confidentiality, contemplated in article 5.1.f) of the RGPD.

Establishing in article 5.1.f) of the aforementioned RGPD that: Personal data

will be (...) f) treated in such a way as to guarantee adequate security of the

personal data, including protection against unauthorized or unlawful processing and

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

appropriate technical or organizational ("integrity and confidentiality").

Duty of confidentiality or secrecy, which constitutes one of the manifestations

essentials of the fundamental right to protection of personal data (article 18.4

EC).

Duty of confidentiality or secrecy incumbent on everyone who intervenes

at any stage of the processing, an obligation that is complementary to the duty to

professional secrecy and that means that they cannot reveal or disclose their

content having the duty to keep them.

v

Article 83.5 a) of the RGPD, considers that the infringement of “the basic principles

costs for treatment, including the conditions for consent under the

articles 5, 6, 7 and 9” is punishable in accordance with section 5 of the aforementioned

Article 83 of the aforementioned Regulation, "with administrative fines of €20,000,000 as

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

maximum of the overall annual total turnover of the previous financial year,

opting for the highest amount.

On the other hand, the LOPDGDD, for prescription purposes, in its article 72 indicates:

“Infringements considered very serious:

1. Based on the provisions of article 83.5 of the Regulation (EU)

2016/679 are considered very serious and the infractions that

suppose a substantial violation of the articles mentioned in that and, in

particularly the following:

a) The processing of personal data violating the principles and guarantees

established in article 5 of Regulation (EU) 2016/679.

(…)”

SAW

Second, it should be noted that the security of personal data

It is regulated in articles 32 of the RGPD.

Article 32 of the RGPD "Security of treatment", establishes that:

"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 availability and access to data

quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and evaluation 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 consideration shall be given to

taking 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 article 32 of the RGPD is typified in the article

83.4.a) of the aforementioned RGPD in the following terms:

"4. Violations of the following provisions will be sanctioned, in accordance

with paragraph 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 8,

11, 25 to 39, 42 and 43.

(…)"

For its part, the LOPDGDD in its article 73, for prescription purposes, qualifies

of "Infringements considered serious":

"Based on the provisions of article 83.4 of Regulation (EU) 2016/679

are considered serious and will prescribe after two years the infractions that suppose a

substantial violation of the articles mentioned therein and, in particular, the

following:

(…)

f) The lack of adoption of those technical and organizational measures that

are appropriate 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.

(…)”

The facts revealed in this claim materialize

in suppose the breach of the technical and organizational measures violating the

data confidentiality.

7th

The GDPR defines personal data security breaches as

“all those violations of security that cause the destruction, loss or

accidental or unlawful alteration of personal data transmitted, stored or processed

otherwise, or unauthorized communication or access to such data”.

From the documentation in the file, there are clear indications of

that the claimed party has violated article 32 of the RGPD, when an incident of

security since through the portal https://konvoko.com, where they are stored

various community documents, and the application that can be downloaded from the

Mobile allows access to these documents made available to neighbors. Nope

However, downloaded the application allows free access, without any kind of

password, being able to view the personal data as there are no security measures

adequate security to prevent indiscriminate access to the information of the

Community of owners.

It should be noted that the RGPD in the aforementioned provision does not establish a list of

the security measures that are applicable according to the data that is

object of treatment, but it establishes that the person in charge and the person in charge of the

treatment will apply technical and organizational measures that are appropriate to the risk

that the treatment entails, taking into account the state of the art, the costs of

application, the nature, scope, context and purposes of the treatment, the risks of

probability and seriousness for the rights and freedoms of the persons concerned.

Likewise, the security measures must be adequate and

proportionate to the detected risk, pointing out that the determination of the measures

technical and organizational information must be carried out taking into account: pseudonymization and

encryption, the ability to ensure the confidentiality, integrity, availability and

resiliency, the ability to restore availability and access to data after a

incident, verification process (not audit), evaluation and assessment of the

effectiveness of the measures.

In any case, when evaluating the adequacy of the level of security,

particularly taking into account the risks presented by the processing of data, such 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 and that could cause damages

physical, material or immaterial.

In this same sense, recital 83 of the RGPD states that:

“(83) In order to maintain security and prevent the treatment from violating the

provided in this Regulation, the person in charge or the person in charge must evaluate

the risks inherent to the treatment and apply measures to mitigate them, such as

encryption. These measures must guarantee an adequate level of security, including

confidentiality, taking into account the state of the art and the cost of its application

regarding the risks and the nature of the personal data that must be

protect yourself. When assessing the risk in relation to data security,

take into account the risks arising from the processing of personal data,
such as the accidental or unlawful destruction, loss or alteration of personal data
transmitted, stored or otherwise processed, or the communication or access is not
authorized to said data, susceptible in particular to cause damages
physical, material or immaterial.
The responsibility of the claimed party is determined by the bankruptcy of
security revealed by the claimant, since it is responsible for taking
decisions aimed at effectively implementing technical measures and
appropriate organizational measures to guarantee a level of security appropriate to the risk
to ensure the confidentiality of the data, restoring its availability and preventing
free access to them.
However, the documentation provided shows that the entity did not
has not only failed to comply with this obligation, but also the adoption of
measures in this regard, except for the cancellation of the company's computer application
hired by the community.
In accordance with the foregoing, it is estimated that the defendant would be the
responsible for the infringement of the RGPD: the violation of article 32, infringement
typified in article 83.4.a).
viii
The defendant alleges that in no way can the Co-
community of Advocacy Owners and that “making decisions aimed at implementing
Effectively promote the appropriate technical and organizational measures to ensure
guarantee a level of security appropriate to the risk”, is the responsibility of the company
owner of the application, because due to its idiosyncrasy as a Community of Owners, it does not
has possibilities to deal with technical or other issues in an application
third-party computing, and therefore, is not responsible for violating article 32 of the RGPD.

However, such an allegation could not be admitted either; the claimed is the

responsible for data processing, in the present case the community of

owners, the natural or legal person or public authority in charge of deciding on

the processing of personal data of individuals. which is responsible for determining

the purposes and means for the treatment, to establish the technical measures and

organizations that guarantee the security of the data, who decides if they want to have

with the help of a data processor, or if you decide to carry out the treatment of

data by itself. In addition, a minimum diligence would have sufficed to verify

that the personal data was exposed to the public

In article 24 of the RGPD, the objectives are indicated in a general way, making

emphasize their obligation to apply the necessary technical and organizational measures

to guarantee compliance with the law in accordance with the provisions of the RGPD.

"1. Taking into account the nature, scope, context and purposes of the

treatment as well as the risks of varying probability and severity for the rights

and freedoms of natural persons, the data controller will apply measures

appropriate technical and organizational measures in order to guarantee and be able to demonstrate that the

processing is in accordance with this Regulation. These measures will be reviewed and

will update when necessary.

2. When they are provided in relation to treatment activities,

The measures mentioned in paragraph 1 shall include the application, by the

responsible for the treatment, of the appropriate data protection policies.

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

certification mechanism approved under article 42 may be used

as elements to demonstrate compliance with the obligations by the

data controller".

IX

Finally, the assumption examined is motivated by the evidence that the

claimed by allowing access through the established application to documents

community, among which are minutes with personal data and situations of

non-payment, there has been a breach of the technical and organizational measures

violating the confidentiality of the data.

Said conduct constitutes the infringement of the provisions of articles 5.1.f) and

32.1 of the GDPR.

However, as pointed out in the motion for a resolution, these

infractions can be sanctioned with a warning in accordance with article

58.2.b) of the RGPD and consider that the administrative fine that could fall with

in accordance with the provisions of article 83.5.a) and 83.4.a) of the RGPD would constitute a burden

disproportionate to the claimant.

At this point, it is necessary to point out that if you do not correct and reiterate the

conduct revealed in the claim and that is the cause of this

procedure, as well as not informing this AEPD of the measures adopted could

proceed to the exercise of possible actions before the person in charge of the treatment to

so that appropriate measures are effectively applied to guarantee the

treatment and confidentiality of personal data and do not return to

incidents such as the one that has given rise to this file, as well as

the provision of supporting evidence of compliance with what is required.

Therefore, in accordance with the applicable legislation and having assessed the criteria for

graduation of sanctions whose existence has been proven,

The Director of the Spanish Data Protection Agency RESOLVES:

FIRST: ADDRESS the COMMUNITY OF OWNERS B.B.B., with NIF ***NIF.1,

for infringement of articles 5.1.f) and 32.1 of the RGPD, typified in articles 83.5.a)

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

14/14

and 83.4.a) of the RGPD, a warning.

SECOND: REQUIRE the COMMUNITY OF OWNERS B.B.B., with NIF

***NIF.1, so that within a month from the notification of this resolution,

proves the adoption of necessary and pertinent measures in accordance with the regulations

tive regarding the protection of personal data in order to avoid that in the

incidents such as those that have given rise to the claim occur again in the future

correcting the effects of its possible infraction, adapting the treatment of the data

of a personal nature to the requirements contemplated in articles 5.1.f), and 32.1 of the

GDPR.

THIRD: NOTIFY this resolution to the OWNER COMMUNITY-

RIOS B.B.B.

In accordance with the provisions of article 50 of the LOPDGDD, 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

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

resents may optionally file an appeal for reconsideration before the Director

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

the day following the notification of this resolution or directly contentious appeal
before the Contentious-Administrative Chamber of the National High Court,
in accordance with the provisions of article 25 and section 5 of the additional provision
Final fourth of Law 29/1998, of July 13, regulating the Contentious Jurisdiction-
administrative, within a period of two months from the day following the notification
tion of this act, as provided for in article 46.1 of the aforementioned Law.
Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the LPACAP,
may provisionally suspend the firm resolution in administrative proceedings if the interested party
do states its intention to file a contentious-administrative appeal. If it is-
In this case, the interested party must formally communicate this fact in writing
addressed to the Spanish Agency for Data Protection, presenting it through the Re-
Electronic registry of the Agency [https://sedeagpd.gob.es/sede-electronica-web/], or to
through any of the other registers provided for in art. 16.4 of the aforementioned Law
39/2015, of October 1. You must also transfer to the Agency the documentation
that proves the effective filing of the contentious-administrative appeal. If the
Agency was not aware of the filing of the contentious-administrative appeal
tive within two months from the day following the notification of this
resolution, would end the precautionary suspension.
Sea Spain Marti
Director of the Spanish Data Protection Agency
C/ Jorge Juan, 6
28001 – Madrid
www.aepd.es
sedeagpd.gob.es