 Procedure No.: PS/00428/2020

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following:

BACKGROUND

FIRST: Ms. A.A.A. (hereinafter, the claimant) dated July 22, 2020

filed a claim with the Spanish Data Protection Agency.

The claim is directed against the Chamber of Urban Property Association of

Burgos and Province with NIF G09460338 (hereinafter, the claimed one).

The claimant states that her next of kin have received telephone calls

requiring them to pay a debt of theirs. Having the claimed, obtained and treated

without consent that data.

It adds that later the respondent sent a document to a family member on the

mentioned debt, and therefore I violate the duty of confidentiality.

And, provide the following documentation:

WhatsApp request sent to the claimant's father.

List of calls made from the switchboard of the claimed party to the father of

the claimant.

Demonstration of the telephone number belonging to the Chamber.

Notice to the father of the claimant who contacted him by telephone and

WhatsApp.

Written proof of the House call to the claimant's aunt.

SECOND: The present claim was transferred to the respondent on 18

September 2020, requiring you to send this document within a month

Agency, information on the causes that have motivated the incidence that has

originated the claim, report on the measures adopted to prevent it from being

similar incidents occur, dates of implementation and controls carried out to

check its effectiveness.

Well, on October 20 of this year, the respondent made the following

statements: "that in the event of non-payment of the lease, the owner

entrusted the defendant with the management of the debt, which is why they were put in

contact with the two tenants, one of them the claimant, with whom they came to

a payment agreement which was breached.

Later, one of the tenants stated that they were going to lend them the money

to pay the debt and provided a third party's telephone number. They made a call to that

telephone by providing another telephone number that turned out to be that of the father of one of the

tenants, with whom the complained party contacted and at his request they sent him

information about said debt.

Faced with the claim made by the tenants, they contacted them and

reported the above.

Likewise, the respondent declares that it has agreed to review the procedure for

action in relation to the personal data of the tenants and have written

a use model for these cases (data not provided directly by the

interested parties) for the best safeguard of the rights of the interested parties, their

intimacy and privacy, and compliance with the duty of information".

THIRD: On December 23, 2020, the Director of the Spanish Agency

of Data Protection agreed to initiate a sanctioning procedure against the claimed party, with in accordance with the provisions of articles 63 and 64 of Law 39/2015, of October 1, of the Common Administrative Procedure of Public Administrations (hereinafter, LPACAP), for alleged violations of articles 5.1 f) and 32 of the RGPD, typified in articles 83.5 a) and 83.4 a) of the RGPD.

FOURTH: Having been notified of the aforementioned initiation agreement, the respondent submitted a written allegations in which, in summary, it stated: "that the facts have their origin in the debt that, for rent and supplies, the claimant maintained with the owner of the home he had been occupying, whose claim and management was entrusted by the property to LA CAMARA. Accredited fact.

It is important to clarify that THE CHAMBER, among others, provides the service of administration and integral management of leases: contracting, maintenance, development, compliance and control of the contractual relationship with the tenant.

The CHAMBER limited itself to complying with the order received from the property, according to the information received, in order to avoid greater damages that would cause the claimant and her partner derived from the possible cut off of the supply electric. Its intention was not to communicate data to third parties or cause damage to the claimant.

On the other hand, in relation to data protection by design and by default, THE CHAMBER contracted the services of the law firm LIFE Abogados, implementing the technical and organizational measures that were considered reasonable commensurate with the risk. Security measures were taken to safeguard the confidentiality of the information, signing the corresponding confidentiality documents with employees and users of ML systems CAMARA, they were instructed and given instructions regarding their functions and obligations for data security, and the document with the policy of use of

the tools made available to users, who signed all the

employees.

In accordance with the principle of proactive responsibility, after mapping data and

risk analysis, the technical and organizational structure of LA CAMARA was designed and

reasonable measures commensurate with the risk to restrict access to the data to

unauthorized persons (user control) and that the data is not accessible to a

indeterminate number of people without human intervention and guarantee their

physical security.

Particularly, in the management of leases and data processing

associated with rental contracts, THE CHAMBER uses the program

computer called GESFINCAS, which can only be accessed by authorized personnel.

For this, there is an access control both to the equipment and to the resources

shared. LA CAMARA users only have access to the resources and

data they need for the development of their functions, control that allows the own

GESFINCAS application.

As proof of all of the above, we attach documents 3 and 4 (document of

confidentiality to which the security policy in data processing is attached

personal and political in the use of the tools made available to the

users. Document 5, technical and organizational structure of THE CHAMBER in the

information storage and processing. As document 6, report of

proactive responsibility of THE CHAMBER (result of the adjustment made by THE

CAMARA to the new regulation on data protection, RGPD).

For this reason, we request the dismissal of this sanctioning procedure and

filing of the proceedings or subsidiarily, the commission of a crime is declared

infringement of art. 5.1 f) RGPD typified in art. 83. 5 a) of the RGPD, and under the

art. 58.2b RGPD the sanction of warning is imposed. Subsidiarily to

above, if the commission of two infractions is maintained, we show our

in accordance with the sanction of warning, considering that, prior to the

initiation of this procedure, this Association has already adopted organizational measures

complementary measures aimed at correcting the facts that are the subject of the complaint and preventing

repeat in the future".

FIFTH: On January 18, 2021, the instructor of the procedure agreed to the

opening of a period of practice tests, considering incorporated the

previous actions E/07100/2020, as well as the documents provided by the

claimed.

SIXTH: On February 8, 2021, a resolution proposal was formulated, proposing that

by the Director of the Spanish Agency for Data Protection to sanction the

Chamber Association of Urban Property of Burgos and Province, with NIF

G09460338, for infringements of articles 5.1 f) and 32 of the RGPD, typified in

Articles 83.5 a) and 83.4 a) of the RGPD respectively.

□

□

for the infringement of article 32 of the RGPD, typified in article 83.4 a) of the

RGPD the sanction that would correspond would be a warning.

for the infringement of article 5.1 f) of the RGPD, typified in article 83.5 a) of the

RGPD the sanction that would correspond would be a warning.

Once the proposed resolution was notified, the respondent has not made any allegations to the

same.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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

FIRST: It is accredited that the respondent sent a copy of the claim for

amount of the claimant to a third party, to whom he informed of the debt contracted by her.

SECOND: WhatsApp confirms the request sent to the claimant's father.

There is a list of calls made from the switchboard of the claimed party to the father of

the claimant.

There is a written proof of the call from the Chamber to the claimant's aunt.

THIRD: The defendant has provided in this sanctioning procedure the

measures that it has adopted, among them it consists:

Confidentiality and professional secrecy agreement.

Policy on the use of technological tools made available to users

users.

Staff security policy for the processing of personal data functions and

user obligations.

Proactive responsibility report.

Duties of the Teleworker in terms of data protection.

Consent to use personal devices for telecommuting.

Organizational technical structure. Files. Organization. Means. Staff.

External companies that process the data.

FOUNDATIONS OF LAW

Yo

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

control, and according to the provisions of articles 47 and 48 of the LOPDGDD, the Director

of the Spanish Agency for Data Protection is competent to initiate and to

resolve this procedure.

II

The defendant is charged with the commission of an infraction for violation of articles

5.1 f) and 32 of the GDPR.

Article 5 establishes the principles that must govern the treatment of

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

The article notes that:

"1. The personal data will be:

(…)

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

In turn, the security of personal data is regulated in article 32 of the

GDPR.

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)

b)

c)

pseudonymization and encryption of personal data;

the ability to ensure the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

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

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 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

of greater 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 71, Violations, states that: "They constitute

infractions the acts and behaviors referred to in sections 4, 5 and 6 of the

Article 83 of Regulation (EU) 2016/679, as well as those that are contrary to the

present organic law".

And in its article 73, for the purposes of prescription, it qualifies as "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:

(…)

g) The violation, as a consequence of the lack of due diligence,

of the technical and organizational measures that have been implemented in accordance with

required by article 32.1 of Regulation (EU) 2016/679".

III

The GDPR defines personal data security breaches as "all

those breaches of security that cause the destruction, loss or alteration

accidental or illicit of personal data transmitted, conserved or treated in another

form, or unauthorized communication or access to said data".

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

claimed has violated article 32 of the RGPD, when there was a breach of

security in their systems by sending a copy of the claim for the amount of the

claimant to a third party, to whom it informs of the debt contracted by the claimant.

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

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

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

apply technical and organizational measures that are appropriate to the risk involved

the treatment, taking into account the state of the art, the application costs, 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 technical measures and organizational must be carried out taking into account: pseudonymization and encryption, capacity to guarantee confidentiality, integrity, availability and resilience, the ability to restore availability and access to data after an incident, process verification (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 provisions of 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 ensure an adequate level of security, including the 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.

IV

Article 72.1.a) of the LOPDGDD states that "according to what is established in the Article 83.5 of Regulation (EU) 2016/679 are considered very serious and will prescribe after three years the infractions that suppose a substantial violation of the articles mentioned therein and, in particular, the following:

a) The processing of personal data violating the principles and guarantees established in article 5 of Regulation (EU) 2016/679.

However, article 58.2 of the RGPD provides the following: "Each authority of control will have all the following corrective powers indicated below: continuation:

(…)

b) sanction any person responsible or in charge of the treatment with warning when the processing operations have violated the provisions of this Regulation;

(…)"

Therefore, the RGPD, without prejudice to the provisions of its article 83, contemplates in its article 58.2 b) the possibility of going to the warning to correct the treatments

personal data that do not meet your expectations.

According to the available evidence, the documentation

provided, it appears that the respondent party sent a copy of the claim of

amount of the claimant to a third party, to whom it informs of the debt contracted by the

claimant, violating the duty of confidentiality, which constitutes, on the part of the

claimed, of two infractions, one against the provisions of article 32 of the RGPD and

another against the provisions of article 5.1 f) of the RGPD, which governs the principles of

integrity and confidentiality of personal data, as well as the responsibility

proactive of the data controller to demonstrate compliance.

These infractions could be sanctioned with a warning. According to

article 58.2.b) of the RGPD, and considering that the administrative fines that could

fall in accordance with the provisions of article 83.5.b) of the RGPD would constitute a

load disproportionate to that claimed.

In this specific case, it has been accredited by virtue of the documents provided with

its allegations to the initial agreement that the respondent has adopted a series of

adequate measures to guarantee the security and confidentiality of the data.

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

graduation of the sanctions whose existence has been proven, the Director of the

Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE the Burgos Urban Property Chamber Association and

Province, with NIF G09460338, for infractions of articles 5.1 f) and 32 of the

RGPD, typified in articles 83.5 a) and 83.4 a) of the RGPD respectively, the

sanctions would be of a warning.

SECOND: NOTIFY this resolution to the Chamber Association of the

Urban Property of Burgos and Province.

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 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.

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 The interested party expresses his intention to file a contentious-administrative appeal. If this is the case, the interested party must formally communicate this fact by writing addressed to the Spanish Agency for Data Protection, presenting it through Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-web/], or 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 proving the effective filing of the contentious appeal-

administrative. If the Agency was not aware of the filing of the appeal

contentious-administrative within a period of 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

938-131120

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es