 File No.: EXP202104953

RESOLUTION OF SANCTIONING PROCEDURE

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

to the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the claiming party), on October 11, 2021,

filed a claim with the Spanish Data Protection Agency. The

The claim is directed against RESIDENCIAS AITA Y AMA BARAKALDO, S.L., with NIF

B95582862 (hereinafter, the claimed party). The reasons on which the claim is based

are the following:

The claimant states that the entity RESIDENCIAS AITA Y AMA BARAKALDO, S.L.

violated the data protection regulations by sending your dismissal letter to all

company workers. According to him, this document was sent to a group of

WhatsApp in which the workers were informed that the ***POSITION.1, the

claimant, had been dismissed, indicating in the message that the

letter of dismissal.

Along with the claim, provide a screenshot of the messaging application

WhatsApp containing the messages object of the claim.

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

December, Protection of Personal Data and Guarantee of Digital Rights

(hereinafter LOPDGDD), said claim was transferred to the claimed party,

to proceed with its analysis and inform this Agency within a month,

of the actions carried out to adapt to the requirements established in the

data protection regulations.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of

October 1, of the Common Administrative Procedure of the Administrations

Public (hereinafter, LPACAP) by electronic notification, was not collected by

the person in charge, within the period of availability, understood as rejected

in accordance with the provisions of art. 43.2 of the LPACAP, dated December 11, 2021,

as stated in the certificate that is in the file.

Although the notification was validly made by electronic means, assuming that

carried out the procedure in accordance with the provisions of article 41.5 of the LPACAP, under

informative, a copy was sent by postal mail that was returned by the Service of

Post office for "absent during delivery hours", leaving a notice in the mailbox. in bliss

notification, they were reminded of their obligation to interact electronically with the

Administration, and was informed of the means of access to said notifications,

reiterating that, henceforth, you will be notified exclusively by means

electronics.

No response has been received to this letter of transfer.

THIRD: On January 11, 2022, in accordance with article 65 of the

LOPDGDD, the admission for processing of the claim presented by the

complaining party.

FOURTH: The General Subdirectorate of Data Inspection proceeded to carry out

of previous investigative actions to clarify the facts in

matter, by virtue of the functions assigned to the control authorities in the

article 57.1 and the powers granted in article 58.1 of the Regulation (EU)

2016/679 (General Data Protection Regulation, hereinafter GDPR), and

in accordance with the provisions of Title VII, Chapter I, Second Section, of the

LOPDGDD, having knowledge of the following extremes:

INVESTIGATED ENTITY

AITA AND AMA BARAKALDO RESIDENCES, S.L. with NIF B95582862, with address at

ALDAPA, 14 BAJO – 48901, BARAKALDO (BISCAY).

RESULT OF INVESTIGATION ACTIONS

The document provided consists of a screenshot of a group of users

of the WhatsApp messaging application, a group of at least 5 members plus the

recipient of the message, according to the information that appears on the screen.

The name of the group is “Aita y Ama”.

The screen print shows a message sent to the aforementioned group by the

contact name "***CONTACT.1" with the following text:

“Hello guys, for your information I have attached the letter of dismissal from A.A.A.. A

As of today, A.A.A. he no longer works at aita y ama. Consequently, neither

is the *** POSITION.1. (…). All the best".

A two-page pdf document can be seen on the screen, as the following message,

referred by the same contact. In the pdf document, the beginning of which appears in

the screen print provided, the AITA RESIDENCE Y

AMA, SL and is addressed to the claimant, not displaying the rest of her

content.

Two requests for information have been issued for the investigation of the facts,

none of them having been collected by the claimed party.

A notice about the closure of the Residence has been found, published in NIUS,

newspaper of CONECTA5 TELECINCO, S.A.U. with the headline 'The Aita residence is closed and

Ama de Barakaldo due to "lack of personnel and the helplessness of the users."

The news is dated 10/13/2021 and contains the following text:

'The Provincial Council of Bizkaia makes this decision after the complaint from the ELA union

which also ensures that "services such as medicine or

Nursing"

The Provincial Council of Bizkaia has decreed the temporary closure of the Residence

Aita and Ama (Iñigo Loyola de Barakaldo Residence) after detecting "several

irregularities" that were denounced by the ELA union.

According to the workers, the managers of the center were committing

infractions such as unfair dismissals, lack of coverage of the

workers, that they cease to provide medical or nursing services or

non-compliance in terms of ratio.

It was in August of this year when ELA informed the Diputación

Foral de Bizkaia the untenable situation of this residence. "Irregularities

occur after the transfer of the residence to a new owner, a situation

that derived in an absolute abandonment of the residents and workers.

After a month and a half of interpellation to the institutions, of insistence, and of

formal and public complaints, the inspection and control service of Bizkaia

confirms the veracity of the facts denounced by ELA and decrees the closure

temporary residence ", they point out in a statement.

For the union, "what happened at the Iñigo de Loyola Residence in Barakaldo is

a clear example that the current care model does not work. The Provincial Council

of Bizkaia is committed to a privatized care model, leaving in the hands of

companies and/or owners taking care of people; companies that prioritize

economic benefit to life.

On the other hand, the Vizcaya Provincial Council plans to "give the explanations

opportune" about this closure in the Health Commission that will be held this

Thursday at the General Meetings.'

On April 21, 2022, there are other news related to the aforementioned

closure, not finding any on its reopening.

On the other hand, searches of telephone numbers of the claimed party and

telephone calls to the numbers found, it is not possible to contact the

claimed entity.

According to news found on the Internet, the Aita y Ama Residence is located

closed.

FIFTH: On July 21, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate disciplinary proceedings against the claimed party,

for the alleged infringement of articles 5.1.f) of the GDPR and 32 of the GDPR, typified

in articles 83.5 and 83.4 of the GDPR, respectively

The startup agreement was sent, in accordance with the rules established in the Law

39/2015, of October 1, of the Common Administrative Procedure of the

Public Administrations (hereinafter, LPACAP), by means of electronic notification,

Although it was not collected by the person in charge, within the period of making it available,

being understood rejected in accordance with the provisions of art. 43.2 of the LPACAP, in

dated August 6, 2022, as stated in the certificate in the file.

The initiation agreement was mailed and returned by the Postal Service by

"absent in distribution", proceeding to its publication in the Official State Gazette, in

dated November 25, 2022, in accordance with the provisions of article 44 of the

Law 39/2015, of October 1, on the Common Administrative Procedure of Admi-

Public administrations.

SIXTH: Notified the aforementioned start agreement in accordance with the rules established in

Law 39/2015, of October 1, on the Common Administrative Procedure of

Public Administrations (hereinafter, LPACAP) and after the period granted

for the formulation of allegations, it has been verified that no allegation has been received

any by the claimed party.

Article 64.2.f) of the LPACAP -provision of which the claimed party was informed

in the agreement to open the procedure - establishes that if no

arguments within the established term on the content of the initiation agreement, when

it contains a precise pronouncement about the imputed responsibility,

may be considered a resolution proposal. In the present case, the agreement of

beginning of the disciplinary file determined the facts in which the

imputation, the infringement of the GDPR attributed to the defendant and the sanction that could

impose. Therefore, taking into consideration that the claimed party has not

made allegations to the agreement to start the file and in attention to what

established in article 64.2.f) of the LPACAP, the aforementioned initiation agreement is

considered in the present case resolution proposal.

In view of all the proceedings, by the Spanish Agency for Data Protection

In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: It is established that the claimed party sent the dismissal letter of the party

complainant to a WhatsApp group in which the workers were informed that

***POINT.1, the claimant, had been dismissed, indicating in the message that

The dismissal letter was attached.

SECOND: There is a screenshot of the WhatsApp messaging application

containing the messages object of the claim.

FUNDAMENTALS OF LAW

Yo

In accordance with the powers that article 58.2 of Regulation (EU) 2016/679

(General Data Protection Regulation, hereinafter GDPR), grants each

control authority and as established in articles 47 and 48.1 of the Law

Organic 3/2018, of December 5, 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: "Procedures

processed by the Spanish Data Protection Agency will be governed by the provisions

in Regulation (EU) 2016/679, in this organic law, by the provisions

regulations dictated in its development and, insofar as they do not contradict them, with character

subsidiary, by the general rules on administrative procedures."

II

previous questions

In the present case, in accordance with the provisions of article 4.1 of the GDPR, there is

the processing of personal data, since RESIDENCIAS

AITA Y AMA BARAKALDO, S.L. is a residence specialized in the care of

older people than for the assistance and management of their services, performs

processing of personal data of its users and employees.

It carries out this activity in its capacity as data controller, since it is

who determines the purposes and means of such activity, by virtue of article 4.7 of the GDPR:

"responsible for the treatment" or "responsible": the natural or legal person, authority

public authority, service or other body that, alone or jointly with others, determines the purposes and

means of treatment; if the law of the Union or of the Member States determines

determines the purposes and means of the treatment, the person in charge of the treatment or the criteria

Specific reasons for their appointment may be established by the Law of the Union or of the

Member states.

Article 4 section 12 of the RGPD defines, in a broad way, the "violations of security"

security of personal data" (hereinafter security breach) as "all

those security violations that cause the destruction, loss or alteration

Accidental or illegal transfer of personal data transmitted, stored or processed in

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

In the present case, there is a personal data security breach in the

circumstances indicated above, categorized as a breach of confidentiality,

whenever the claimed party has disclosed information and data of a personal nature

to third parties, without the express consent of the owner of said data, by sending a

WhatsApp messaging app user group, group of at least 5

members plus the recipient of the message, the dismissal letter of the complaining party,

in which you can see your full postal address and the reason for the cessation of the

employment relationship.

According to GT29, a "Breach of confidentiality" occurs when there is

an unauthorized or accidental disclosure of personal data, or access to it

themselves.

It should be noted that the identification of a security breach does not imply the impossibility

sanction directly by this Agency, since it is necessary to analyze the

diligence of managers and managers and security measures applied.

Within the principles of treatment provided for in article 5 of the GDPR, the

integrity and confidentiality of personal data is guaranteed in section 1.f)

of article 5 of the GDPR. For its part, the security of personal data comes

regulated in articles 32, 33 and 34 of the GDPR, which regulate the security of the

treatment, the notification of a breach of the security of personal data to

the control authority, as well as the communication to the interested party, respectively.

II

Article 5.1.f) of the GDPR

Article 5.1.f) of the GDPR establishes the following:

"Article 5 Principles relating to treatment:

1. Personal data will be:

(…)

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

personal data, including protection against unauthorized or unlawful processing and against

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

or organizational procedures (“integrity and confidentiality”).”

In relation to this principle, Recital 39 of the aforementioned GDPR states that:

“[…]Personal data must be processed in a way that guarantees security and

appropriate confidentiality of personal data, including to prevent access

or unauthorized use of said data and of the equipment used in the treatment”.

The documentation in the file offers clear indications that the

claimed violated article 5.1 f) of the GDPR, principles relating to treatment.

In the present case, and in the absence of a response from the claimed party, it can be

verify, according to the documentation provided by the claimant, an impression of

screen of a group of users of the WhatsApp messaging application, group of

at least 5 members plus the recipient of the message. The name of the group is “Aita y

Mistress."

On the screen print a message can be seen, in which the cause of the termination is stated

of the employment relationship, sent to the aforementioned group by the contact named

"***CONTACT.1" with the following text:

“Hello guys, for your information I have attached the letter of dismissal from A.A.A.. A

As of today, A.A.A. he no longer works at aita y ama. Consequently, neither

is the *** POSITION.1. (…). All the best".

A two-page pdf document can be seen on the screen, as the following message,

referred by the same contact. In the pdf document, the beginning of which appears in

the screen print provided, the AITA RESIDENCE Y

AMA, SL and is addressed to the claimant. Also, you can view the

Full mailing address of the claimant.

The known facts constitute, on the part of the defendant, in his capacity as

responsible for the aforementioned processing of personal data, a violation of the

principle of confidentiality, by disseminating this information among employees without

certify that it had obtained the consent of the complaining party for that

specific treatment.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Consequently, it is considered that the accredited facts are constitutive of

infringement, attributable to the claimed party, due to violation of article 5.1.f) of the

GDPR.

Classification of the infringement of article 5.1.f) of the GDPR

IV.

The aforementioned infringement of article 5.1.f) of the GDPR supposes the commission of the infringements

typified in article 83.5 of the GDPR that under the heading "General conditions

for the imposition of administrative fines" provides:

Violations of the following provisions will be sanctioned, in accordance with the

paragraph 2, with administrative fines of maximum EUR 20,000,000 or,

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

total annual global business volume of the previous financial year, opting for

the highest amount:

the basic principles for the treatment, including the conditions for the

to)

consent under articles 5, 6, 7 and 9; (…)"

In this regard, the LOPDGDD, in its article 71 "Infractions" establishes that

"The acts and behaviors referred to in sections 4,

5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that result

contrary to this organic law".

For the purposes of the limitation period, article 72 "Infractions considered very

serious" of the LOPDGDD indicates:

"1. Based on what is established in article 83.5 of Regulation (EU) 2016/679,

are considered very serious and will prescribe after three years the infractions that

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

following:

a) The processing of personal data in violation of the principles and guarantees

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

V

GDPR Article 32

Article 32 of the GDPR, security of treatment, establishes the following:

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

nature, scope, context and purposes of processing, 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 and

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

which may include, among others:

a) the 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 assessment of effectiveness

technical and organizational measures to guarantee the safety of the

treatment.

2. When evaluating the adequacy of the security level, particular consideration will be given to

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

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

personal information transmitted, preserved or processed in another way, or the communication or

unauthorized access to such data.

3. Adherence to an approved code of conduct pursuant to 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 controller and the processor shall take measures to ensure that

any person acting under the authority of the controller or processor and

have access to personal data can only process such data by following

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.

Recital 74 of the GDPR establishes:

"The responsibility of the data controller must be established for

any processing of personal data carried out by himself or on his behalf. In

In particular, the person responsible must be obliged to apply timely and effective measures

and must be able to demonstrate the compliance of the processing activities with the

this Regulation, including the effectiveness of the measures. These measures must have

into account the nature, scope, context and purposes of the processing, as well as the

risk to the rights and freedoms of natural persons.”

Since the use of WhatsApp is common for communication and sending

documents or images of documents, it must be taken into account to whom they are sent

messages when personal data is included in said messages, given that if

These data do not belong to the person who sends the message or the recipient of these, there must be

a justification for sending personal data to third parties by WhatsApp.

The facts revealed imply the lack of technical measures and

organizational by enabling the display of personal data of the claimant

with the consequent lack of diligence by the person in charge, allowing unauthorized access

authorized by third parties.

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

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

of treatment, but it 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 processing, probability risks

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

In addition, security measures must be adequate and proportionate to the

detected risk, noting that the determination of the technical measures and

organizational procedures must be carried out taking into account: pseudonymization and encryption, the

ability to ensure 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 security level,

particular account of the risks presented by data processing, such as

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

personal information transmitted, preserved or processed in another way, or the communication or

unauthorized access to said data and that could cause damages

physical, material or immaterial.

In this sense, recital 83 of the GDPR states that:

"(83) In order to maintain security and prevent processing from infringing what

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

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

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 nature of the personal data to be

protect yourself. When assessing risk in relation to data security, considerations should be

take into account the risks arising from the processing of personal data,

such as the destruction, loss or accidental or unlawful alteration of personal data

transmitted, stored or processed in another way, or communication or access not

authorized to said data, susceptible in particular to cause damages

physical, material or immaterial.

The responsibility of the defendant is determined by the lack of measures of

security, since it is responsible for making decisions aimed at implementing

effectively the appropriate technical and organizational measures to guarantee a

level of security appropriate to the risk to ensure the confidentiality of the data,

restoring their availability and preventing access to them in the event of an incident

physical or technical

Therefore, the accredited facts constitute an infraction, attributable to the

claimed party, for violation of article 32 GDPR.

Classification of the infringement of article 32 of the GDPR

SAW

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

The aforementioned infringement of article 32 of the GDPR supposes the commission of the infringements

typified in article 83.4 of the GDPR that under the heading "General conditions

for the imposition of administrative fines" provides:

Violations of the following provisions will be sanctioned, in accordance with the

paragraph 2, with administrative fines of maximum EUR 10,000,000 or,

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

total annual global business volume of the previous financial year, opting for

the highest amount:

to)

the obligations of the controller and the person in charge under articles 8,

11, 25 to 39, 42 and 43; (…)"

In this regard, the LOPDGDD, in its article 71 "Infractions" establishes that

"The acts and behaviors referred to in sections 4,

5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that result

contrary to this organic law".

For the purposes of the limitation period, article 73 "Infractions considered serious"

of the LOPDGDD indicates:

"Based on what is established in 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 ensure a level of security appropriate to the

risk of treatment, in the terms required by article 32.1 of the

Regulation (EU) 2016/679."

VII

Responsibility

Establishes Law 40/2015, of October 1, on the Legal Regime of the Public Sector, in

Chapter III relating to the "Principles of the Power to sanction", in article 28

under the heading "Responsibility", the following:

"1. They may only be penalized for acts constituting an administrative offense

physical and legal persons, as well as, when a Law recognizes their capacity to

act, the affected groups, the unions and entities without legal personality and the

independent or autonomous patrimonies, which are responsible for them

title of fraud or fault."

Lack of diligence in implementing appropriate security measures

with the consequence of the breach of the principle of confidentiality constitutes the

element of guilt.

VIII

Sanction

In order to determine the administrative fine to be imposed, the

provisions of articles 83.1 and 83.2 of the GDPR, precepts that state:

"1. Each control authority will guarantee that the imposition of fines

administrative proceedings under this article for violations of this

Regulations indicated in sections 4, 5 and 6 are in each individual case

effective, proportionate and dissuasive.

2. Administrative fines will be imposed, depending on the circumstances of each

individual case, in addition to or in lieu of the measures contemplated in

Article 58, paragraph 2, letters a) to h) and j). When deciding to impose a fine

administration and its amount in each individual case shall be duly taken into account:

a) the nature, seriousness and duration of the offence, taking into account the nature

nature, scope or purpose of the processing operation in question, as well as the number

number of interested parties affected and the level of damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the person in charge or in charge of the treatment to

settle the damages suffered by the interested parties;

d) the degree of responsibility of the person in charge or of the person in charge of the treatment, habi-

gives an account of the technical or organizational measures that have been applied by virtue of the

articles 25 and 32;

e) any previous infringement committed by the controller or processor;

f) the degree of cooperation with the supervisory authority in order to remedy the

infringement and mitigate the possible adverse effects of the infringement;

g) the categories of personal data affected by the infringement;

h) the way in which the supervisory authority became aware of the infringement, in particular

determine whether the controller or processor notified the infringement and, if so, to what extent

gives; i) when the measures indicated in article 58, paragraph 2, have been ordered

given previously against the person in charge or the person in charge in relation to

the same matter, compliance with said measures;

j) adherence to codes of conduct under article 40 or to certification mechanisms.

fications approved in accordance with article 42,

k) any other aggravating or mitigating factor applicable to the circumstances of the case,

as the financial benefits obtained or the losses avoided, directly or indirectly.

mind, through infraction."

For its part, article 76 "Sanctions and corrective measures" of the LOPDGDD

has:

"1. The sanctions provided for in sections 4, 5 and 6 of article 83 of the Regulation

(UE) 2016/679 will be applied taking into account the graduation criteria

established in section 2 of said article.

2. In accordance with the provisions of article 83.2.k) of Regulation (EU) 2016/679

may also be taken into account:

a) The continuing nature of the offence.

b) Linking the activity of the offender with the performance of processing

of personal data.

c) The benefits obtained as a consequence of the commission of the infraction.

d) The possibility that the conduct of the affected party could have led to the

commission of the offence.

e) The existence of a merger process by absorption after the commission

of the infringement, which cannot be attributed to the absorbing entity.

f) The affectation of the rights of minors.

g) Have, when it is not mandatory, a data protection delegate

h) The submission by the person in charge or in charge, with character

voluntary, alternative conflict resolution mechanisms, in those

cases in which there are controversies between those and any

interested."

data.

Considering the exposed factors, the valuation that reaches the amount of the fine

is €2,000 for violation of article 5.1 f) of the GDPR, regarding the violation of the

principle of confidentiality and €1,500 for violation of article 32 of the aforementioned

GDPR, regarding the security of personal data processing.

IX

Measures

Likewise, it is appropriate to impose the corrective measure described in article 58.2.d) of the

GDPR and order the claimed party to, within a month, establish the measures

Adequate security measures so that the treatments are adapted to the requirements

contemplated in articles 5.1 f) and 32 of the GDPR, preventing them from occurring if

similar situations in the future.

The text of the resolution establishes which have been the infractions committed and

the facts that have given rise to the violation of the regulations for the protection of

data, from which it is clearly inferred what are the measures to adopt, without prejudice

that the type of procedures, mechanisms or concrete instruments for

implement them corresponds to the sanctioned party, since it is responsible for the

treatment who fully knows its organization and has to decide, based on the

proactive responsibility and risk approach, how to comply with the GDPR and the

LOPDGDD.

Therefore, in accordance with the applicable legislation and assessed the criteria of

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

Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE RESIDENCIAS AITA Y AMA BARAKALDO, S.L., with NIF

B95582862,

-for an infringement of article 5.1.f) of the GDPR, classified in accordance with the provisions of article

Article 83.5 of the GDPR, classified as very serious for the purposes of prescription in the

article 72.1 a) of the LOPDGDD, a fine of €2,000.

-for a violation of article 32 of the GDPR, classified in accordance with the provisions of article

article 83.4 of the GDPR, classified as serious for the purposes of prescription in article

73 f) of the LOPDGDD, a fine of €1,500.

SECOND: REQUEST RESIDENCIAS AITA Y AMA BARAKALDO, S.L., with NIF

B95582862, that implements, within a month, the necessary corrective measures

to adapt its actions to the personal data protection regulations, which

prevent the repetition of similar events in the future, as well as to inform this

Agency, within the same period, on the measures adopted.

THIRD: NOTIFY this resolution to AITA AND AMA RESIDENCES

BARAKALDO, S.L.

FOURTH: Warn the sanctioned party that he must enforce the sanction imposed

Once this resolution is enforceable, in accordance with the provisions of Article

art. 98.1.b) of Law 39/2015, of October 1, on Administrative Procedure

Common of Public Administrations (hereinafter LPACAP), within the payment period

voluntary established in art. 68 of the General Collection Regulations, approved

by Royal Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003,

of December 17, by means of its income, indicating the NIF of the sanctioned and the number

of procedure that appears in the heading of this document, in the account

restricted number ES00 0000 0000 0000 0000 0000, open in the name of the Agency

Spanish Data Protection Agency at the bank CAIXABANK, S.A.. In the event

Otherwise, it will proceed to its collection in the executive period.

Once the notification has been received and once executed, if the execution date is

between the 1st and 15th of each month, both inclusive, the term to make the payment

voluntary will be until the 20th day of the following or immediately following business month, and if

between the 16th and the last day of each month, both inclusive, the payment term

It will be until the 5th of the second following or immediately following business month.

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

Resolution will be made public once the interested parties have been notified.

Against this resolution, which puts an end to the administrative process 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 reversal before the

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

count 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 for in article 46.1 of the

referred Law.

Finally, it is noted 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 through

writing addressed to the Spanish Data Protection Agency, presenting it through

of the Electronic Registry of the Agency [https://sedeagpd.gob.es/sede-electronica-

web/], or through any of the other registries 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 proceedings within a period of two months from the day following the

Notification of this resolution would terminate the precautionary suspension.

Mar Spain Marti

Director of the Spanish Data Protection Agency

938-120722

28001 – Madrid

www.aepd.es

sedeagpd.gob.es