 File No.: PS/00420/2021

RESOLUTION OF TERMINATION OF THE PROCEDURE FOR PAYMENT

VOLUNTEER

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

to the following

BACKGROUND

FIRST: On April 18, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate sanctioning proceedings against BANCO BILBAO

VIZCAYA ARGENTARIA, S.A. (hereinafter, the claimed party), through the Agreement

which is transcribed:

<<

File No.: PS/00420/2021

AGREEMENT TO START A SANCTION PROCEDURE

Of the actions carried out by the Spanish Data Protection Agency and in

based on the following

FACTS

FIRST: A.A.A. (hereinafter, the complaining party) dated May 1, 2021

filed a claim with the Spanish Data Protection Agency. The

claim is directed against BANCO BILBAO VIZCAYA ARGENTARIA, S.A. with CIF

A48265169 (hereinafter, the BBVA). The grounds on which the claim is based are

following:

On January 7, 2021, a person unknown to her, made at an ATM

from the entity claimed an income from the rental of an apartment that the party

claimant has leased. As the cashier did not provide any supporting document of the

income, said third party addressed a person from the office who gave him a

document stating the balance of the account of the claimant. As a result of

occurred, contact the office and apologize for the mistake. File claim

in writing before the entity, on January 18, 2021 and receives a response, on the date

February 10, 2021, indicating that, after initiating the pertinent inquiries to

clarify the facts, adopted the appropriate measures, and that they know that the

Those responsible for the affected office apologized for what had happened.

Together with the notification, it provides a document justifying the payment made, where

The balance of the account is recorded, with the stamp of the office dated January 7, 2021,

written claim and response from the claimed entity.

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), said claim was transferred to BBVA so that it

proceed to its analysis and inform this Agency within a month of the

actions carried out to adapt to the requirements set forth in the regulations of

Data Protection.

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), was collected on 06/02/2021 as recorded in the

acknowledgment of receipt that works in the file.

On 07/13/2021, this Agency received a written response indicating:

“On January 7, a person went to the BBVA branch ***OFICINA.1 to

make a cash deposit in the account of Mrs. A.A.A. in concept <<rental

January XXXXXXXXX>>. Since the ATM could not issue proof of

the operation in paper format, said person went to the cash desk and the employee

of BBVA I gave him, by mistake, a document justifying the payment where, in addition,

The balance in Mrs. A.A.A.'s account appeared.

It is true that the cashier at the BBVA branch ***OFFICE.1 committed a

punctual and human error by not deleting the amount of the balance of the account of Mrs.

A.A.A. BBVA regrets the error and informs this Agency that at the same time

that Mrs. A.A.A. contacted the office to ask for explanations for what

happened, he apologized for it, being unable to do more than reiterate his

apologize in writing 8/6/2021”

With the answer, BBVA provides a document, addressed to the complaining party, in which

state that they regret the mistake, apologize, and inform him that they have taken

measures so that it does not happen again.

THIRD: On August 1, 2021, in accordance with article 65 of the

LOPDGDD, the claim filed by the claimant was admitted for processing.

FOUNDATIONS OF LAW

Yo

Competition

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

European Parliament and of the Council of April 27, 2016 on the protection of

individuals with regard to the processing of personal data and the free

circulation of these data (RGPD) recognizes each control authority, and according to what

established in articles 47 and 48 of the LOPDGDD, the Director of the Agency

Spanish Data Protection is competent to initiate and resolve this

process.

II

Previous issues

Article 4 paragraph 12 of the RGPD defines, in a broad way, the "violations of security of personal data" (hereinafter security breach) as "all those breaches of security that cause the destruction, loss or alteration accidental or illicit of personal data transmitted, conserved or processed in another form, or unauthorized communication or access to said data."

In the present case, there is a security breach of personal data in the circumstances indicated above, categorized as a breach of confidentiality, when have been provided to a third person, unrelated to the claimant, the balance of their Bank account.

It should be noted that the identification of a security breach does not imply the imposition of a sanction directly by this Agency, since it is necessary analyze the diligence of those responsible and in charge and the security measures applied.

Within the principles of treatment provided for in article 5 of the RGPD, the integrity and confidentiality of personal data is guaranteed in section 1.f) of article 5 of the RGPD. For its part, the security of personal data comes regulated in articles 32, 33 and 34 of the RGPD, which regulate the security of the treatment, notification of a violation of the security of personal data to the control authority, as well as the communication to the interested party, respectively.

III

Article 5.1.f) of the RGPD

Article 5.1.f) “Principles related to treatment” of the RGPD establishes:

"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 processing or

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

of appropriate technical or organizational measures ("integrity and

confidentiality”).”

In the present case, it is stated that the personal data of the complaining party,

in the BBVA database, were unduly exposed to a third party, since by

provide you with the required document, proof of the deposit made into the account, you will be

also provided the balance of the account, of which the claimant was the holder, data

that should have been deleted or anonymised.

In accordance with the evidence available in this agreement of

initiation of the sanctioning procedure, and without prejudice to what results from the

instruction, it is considered that the known facts could constitute a

infringement, attributable to BBVA, for violation of article 5.1.f) of the RGPD.

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

IV

If confirmed, the aforementioned infringement of article 5.1.f) of the RGPD could lead to the commission of the offenses typified in article 83.5 of the RGPD that under the The heading "General conditions for the imposition of administrative fines" provides:

“The infractions of the following dispositions will be sanctioned, in accordance with the paragraph 2, with administrative fines of a maximum of EUR 20,000,000 or, in the case of a company, an amount equivalent to a maximum of 4% of the global total annual turnover of the previous financial year, opting for the largest amount:

a) the basic principles for the treatment, including the conditions for the consent under articles 5, 6, 7 and 9; (…)”

In this regard, the LOPDGDD, in its article 71 "Infringements" 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 “Infringements considered very serious” of the LOPDGDD indicates:

"1. Based on the provisions of article 83.5 of Regulation (EU) 2016/679, 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. (…)”

Sanction for the infringement of article 5.1.f) of the RGPD

v

For the purposes of deciding on the imposition of an administrative fine and its amount, accordance with the evidence available at the present time.

agreement to initiate sanctioning proceedings, and without prejudice to what results from the

investigation, the infringement in question is considered to be serious for the purposes of

RGPD and that it is appropriate to graduate the sanction to be imposed in accordance with the following

criteria established by article 83.2 of the RGPD:

As aggravating factors:

-The degree of responsibility of the person in charge or of the person in charge of the treatment,

taking into account the technical or organizational measures that they have applied in

under articles 25 and 32. Art. 83.2.d).

BBVA, as data controller, has to implement measures

adequate to avoid the exposure of personal data to third parties not

authorized. Given that in the present case there has been a gap of

confidentiality, it can be assumed that no measures had been taken

appropriate.

Likewise, it is considered appropriate to graduate the sanction to be imposed in accordance with the

following criteria established in section 2 of article 76 “Sanctions and measures

corrective measures” of the LOPDGDD:

As aggravating factors:

-The link between the activity of the offender and the performance of

personal data processing. (Art. 76.2.b).

The activity of BBVA, a financial institution, and the high number of customers

with which it has, entails the handling of a large number of data

personal. This implies that they have sufficient experience and should have

with the adequate knowledge for the treatment of said data.

The balance of the circumstances contemplated in article 83.2 of the RGPD and the

Article 76.2 of the LOPDGDD, with respect to the infraction committed by violating the

established in article 5.1.f) of the RGPD, allows initially setting a penalty of

€50,000 (fifty thousand euros).

SAW

Article 32 of the GDPR

Article 32 “Security of treatment” of the RGPD establishes:

"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 guarantee the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

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

quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and 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 account shall be taken of

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

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

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

unauthorized access to said data.

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

certification mechanism approved under article 42 may serve as an element

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

present article.

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

any person acting under the authority of the person in charge or the person in charge and

has access to personal data can only process said data following

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

the Union or the Member States.

In the present case, at the time the breach occurred, BBVA did not have

adequate technical and organizational measures to prevent the balance of the account

of the complaining party was visible to the person who requested proof of the

income made in said account, data that in no case should have been provided.

In accordance with the evidence available in this agreement of

initiation of the sanctioning procedure, and without prejudice to what results from the

instruction, it is considered that the known facts could constitute a

infringement, attributable to BBVA, for violation of article 32 of the RGPD.

Classification of the infringement of article 32 of the RGPD

7th

If confirmed, the aforementioned violation of article 32 of the RGPD could lead to the

commission of the offenses typified in article 83.4 of the RGPD that under the

The heading "General conditions for the imposition of administrative fines" provides:

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

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; (…)”

In this regard, the LOPDGDD, in its article 71 "Infringements" 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 “Infringements considered serious”

of the LOPDGDD indicates:

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

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 an adequate level of security when

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

Regulation (EU) 2016/679.

(…)

Sanction for the infringement of article 32 of the RGPD

viii

For the purposes of deciding on the imposition of an administrative fine and its amount,

accordance with the evidence available at the present time.

agreement to initiate sanctioning proceedings, and without prejudice to what results from the

investigation, the infringement in question is considered to be serious for the purposes of

RGPD and that it is appropriate to graduate the sanction to be imposed in accordance with the criteria that

establishes article 83.2 of the RGPD:

Likewise, it is considered appropriate to graduate the sanction to be imposed in accordance with the

following criteria established in section 2 of article 76 “Sanctions and measures

corrective measures” of the LOPDGDD:

As aggravating factors:

-The link between the activity of the offender and the performance of

personal data processing. (Art. 76.2.b).

The activity of BBVA, a financial institution, and the high number of customers

with which it has, entails the handling of a large number of data

personal. This implies that they have sufficient experience and should have

with the adequate knowledge for the treatment of said data.

The balance of the circumstances contemplated in article 83.2 of the RGPD and the

Article 76.2 of the LOPDGDD, with respect to the infraction committed by violating the

established in article 32 of the RGPD, allows initially setting a penalty of

€30,000 (thirty thousand euros).

IX

Imposition of measures

Among the corrective powers provided in article 58 "Powers" of the RGPD, in the

Section 2.d) establishes that each control authority may “order the

responsible or in charge of the treatment that the treatment operations are

comply with the provisions of this Regulation, where appropriate, in a

certain manner and within a specified period…”.

The Spanish Agency for Data Protection in the resolution that puts an end to the

This procedure may order the adoption of measures, as established

in article 58.2.d) of the RGPD and in accordance with what is derived from the instruction

of the procedure, if necessary, in addition to sanctioning with a fine.

Therefore, in accordance with the foregoing, by the Director of the Agency

Spanish Data Protection,

HE REMEMBERS:

FIRST: START SANCTION PROCEDURE against BANCO BILBAO VIZCAYA

ARGENTARIA, S.A., with CIF A48265169, for the alleged violation of Article 5.1.f)

of the RGPD and Article 32 of the RGPD, typified in Article 83.5 of the RGPD and Article

83.4, respectively, of the GDPR.

SECOND: APPOINT B.B.B. and, as secretary, to C.C.C.,

indicating that any of them may be challenged, as the case may be, in accordance with

established in articles 23 and 24 of Law 40/2015, of October 1, on the Regime

Legal Department of the Public Sector (LRJSP).

THIRD: INCORPORATE to the disciplinary file, for evidentiary purposes, the

claim filed by the claimant and its documentation, as well as the

documents obtained and generated by the Subdirectorate General for Inspection of

Data in the actions prior to the start of this sanctioning procedure.

FOURTH: THAT for the purposes provided in art. 64.2 b) of Law 39/2015, of 1

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

sanction that could correspond would be 50,000 euros for the infraction of the article

5.1.f) of the RGPD, and 30,000 euros for the infringement of article 32 of the RGPD, without

prejudice to what results from the instruction.

FIFTH: NOTIFY this agreement to BANCO BILBAO VIZCAYA

ARGENTARIA, S.A., with CIF A48265169, granting a hearing period of ten

working days to formulate the allegations and present the evidence that it considers

convenient. In your brief of allegations you must provide your NIF and the number of

procedure at the top of this document.

If within the stipulated period it does not make allegations to this initial agreement, the same

may be considered a resolution proposal, as established in article

64.2.f) of Law 39/2015, of October 1, of the Common Administrative Procedure of

Public Administrations (hereinafter, LPACAP).

In accordance with the provisions of article 85 of the LPACAP, you may recognize your

responsibility within the term granted for the formulation of allegations to the

this initiation agreement; which will entail a reduction of 20% of the

sanction to be imposed in this proceeding. With the application of this

reduction, the sanction would be established at 40,000 euros for the infraction of the

article 5.1.f) of the RGPD, and 24,000 euros for the infringement of article 32 RGPD

(64,000 euros in total), resolving the procedure with the imposition of this

sanction.

Similarly, you may, at any time prior to the resolution of this

procedure, carry out the voluntary payment of the proposed sanction, which

will mean a reduction of 20% of its amount. With the application of this reduction,

the sanction would be established at 40,000 euros for the infraction of article 5.1.f) of the

RGPD, and 24,000 euros for the infringement of article 32 RGPD (64,000 euros in total),

and its payment will imply the termination of the procedure.

The reduction for the voluntary payment of the penalty is cumulative with the corresponding

apply for the acknowledgment of responsibility, provided that this acknowledgment

of the responsibility is revealed within the period granted to formulate

arguments at the opening of the procedure. The voluntary payment of the referred amount

in the previous paragraph may be done at any time prior to the resolution. In

In this case, if it were appropriate to apply both reductions, the amount of the penalty would be

established at 30,000 euros for the infringement of article 5.1.f) of the RGPD, and 18,000

euros for the infringement of article 32 of the RGPD, (48,000 euros in total).

In any case, the effectiveness of any of the two reductions mentioned will be

conditioned to the abandonment or renunciation of any action or resource in via

administrative against the sanction.

In case you chose to proceed to the voluntary payment of any of the amounts

indicated above (64,000 euros or 48,000 euros), you must make it effective

by depositing it in account number ES00 0000 0000 0000 0000 0000 open to

name of the Spanish Agency for Data Protection in the bank

CAIXABANK, S.A., indicating in the concept the reference number of the

procedure that appears in the heading of this document and the cause of

reduction of the amount to which it is accepted.

Likewise, you must send proof of payment to the General Subdirectorate of

Inspection to proceed with the procedure in accordance with the quantity

entered.

The procedure will have a maximum duration of nine months from the

date of the start-up agreement or, where appropriate, of the draft start-up agreement.

Once this period has elapsed, it will expire and, consequently, the file of

performances; in accordance with the provisions of article 64 of the LOPDGDD.

Finally, it is pointed out that in accordance with the provisions of article 112.1 of the

LPACAP, there is no administrative appeal against this act.

Sea Spain Marti

Director of the Spanish Data Protection Agency

935-150322

>>

SECOND: On April 28, 2022, the claimed party has proceeded to pay

the sanction in the amount of 48,000 euros making use of the two reductions

provided for in the Start Agreement transcribed above, which implies the

acknowledgment of responsibility.

THIRD: The payment made, within the period granted to formulate allegations to

the opening of the procedure, entails the waiver of any action or resource in via

administrative action against the sanction and acknowledgment of responsibility in relation to

the facts referred to in the Initiation Agreement.

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

control authority and as established in articles 47 and 48.1 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

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

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

regulations issued in its development and, as long as they do not contradict them, with a

subsidiary, by the general rules on administrative procedures.”

II

Article 85 of Law 39/2015, of October 1, on Administrative Procedure

Common to Public Administrations (hereinafter, LPACAP), under the rubric

"Termination in sanctioning procedures" provides the following:

"1. Started a sanctioning procedure, if the offender acknowledges his responsibility,

the procedure may be resolved with the imposition of the appropriate sanction.

2. When the sanction is solely pecuniary in nature or it is possible to impose a

pecuniary sanction and another of a non-pecuniary nature, but the

inadmissibility of the second, the voluntary payment by the alleged perpetrator, in

any time prior to the resolution, will imply the termination of the procedure,

except in relation to the replacement of the altered situation or the determination of the

compensation for damages caused by the commission of the infringement.

3. In both cases, when the sanction is solely pecuniary in nature, the

competent body to resolve the procedure will apply reductions of, at least,

20% of the amount of the proposed sanction, these being cumulative with each other.

The aforementioned reductions must be determined in the notification of initiation

of the procedure and its effectiveness will be conditioned to the withdrawal or resignation of

any administrative action or recourse against the sanction.

The reduction percentage provided for in this section may be increased

regulations."

According to what was stated,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: TO DECLARE the termination of procedure PS/00420/2021, of

in accordance with the provisions of article 85 of the LPACAP.

SECOND: NOTIFY this resolution to BANCO BILBAO VIZCAYA

ARGENTARIA, S.A.

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 as prescribed by

the art. 114.1.c) of Law 39/2015, of October 1, on Administrative Procedure Common of the Public Administrations, the interested parties may file an appeal contentious-administrative before the Contentious-administrative Chamber of the National Court, in accordance with the provisions of article 25 and section 5 of the fourth additional provision of Law 29/1998, of July 13, regulating the Contentious-Administrative Jurisdiction, within a period of two months from the day following the notification of this act, as provided in article 46.1 of the aforementioned Law.

Sea Spain Marti

Director of the Spanish Data Protection Agency

936-240122

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es