 File No.: PS/00362/2021

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 July 27, 2021, 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:

<<

Procedure No.: PS/00362/2021

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 claimant) dated March 25, 2020

filed a claim with the Spanish Data Protection Agency.

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

with NIF A48265169 (hereinafter, the claimed).

The reasons on which the claim is based are that the respondent provides details of the last movements of the Affinity Card through a service system automated telephone call on the telephone ***TELÉFONO.1 in which only as identification data the client's ID.

It is stated by the claimant that the entity claimed does not adopt any other security measure to confirm the identity of the client so that any person can call, give a DNI number and obtain information associated with that DNI, without verifying that the caller is the holder of said document identification.

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/03724/2020, transfer of said claim to the claimant on June 8, 2020, so that he could proceed with his analysis and report to this Agency within a month, of the actions carried out carried out to adapt to the requirements set forth in the data protection regulations.

Despite the nature of this requirement, which, as indicated in article 65.4 of the LOPDGDD, is optional and prior to the start of any procedure, the September 25, 2020, the entity claimed in response to the requirement of this Agency, states that the Agency's letter has not indicated the deadline for respond, which implies an error in the processing of the procedure, which is why that based on article 76.2 of Law 39/2015 of Common Administrative Procedure of the Public Administrations, requests that the procedure be paralyzed, until said error is corrected and you are notified again of said request for information.

THIRD: On December 4, 2020, the Director of the Spanish Agency for Data Protection agreed to admit for processing the claim presented by the claimant.

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

documents provided by the claimant, the Subdirectorate General for Inspection of

Data proceeded to carry out preliminary investigation actions for the

clarification of the facts in question, by virtue of the investigative powers

granted to the control authorities in article 57.1 of the Regulation (EU)

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

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

Organic 3/2018, of December 5, on the Protection of Personal Data and guarantee of

digital rights (hereinafter LOPDGDD).

As a result of the research actions carried out, it is found that the

responsible for the treatment is the claimed.

In addition, the following extremes are noted:

On December 10, 2020, a request for information is sent to BANK

BILBAO VIZCAYA ARGENTARIA, S.A. using several ways:

 Electronically through notific@, a system that allows proof that the

notification has been delivered on December 16, 2020, but no

receive reply.

 By post, but no reply is received.

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

Article 58 of the GDPR states:

"two. Each supervisory authority will have all of the following corrective powers listed below:

(…)

i) impose an administrative fine under article 83, in addition to or instead of the measures mentioned in this section, according to the circumstances of each particular case;

(…)"

The RGPD establishes in article 5 of 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) 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").

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

RGPD, where it is established 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;

the ability to ensure the confidentiality, integrity, availability and

a)

permanent resilience of treatment systems and services;

the ability to restore availability and access to personal data

b)

quickly in the event of a physical or technical incident;

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

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

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

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

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

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

unauthorized access to said data.

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

certification mechanism approved under article 42 may serve as an element

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

present article.

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

any person acting under the authority of the 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.

The violation of article 32.1 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 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 of the person in charge pursuant to articles 8, 11, 25 a

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,

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 result

appropriate to guarantee a level of security appropriate to the risk of the treatment,

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

III

The RGPD in the aforementioned article 32, does not establish a list of security measures

that are applicable according to the data being processed, but

that establishes that the person in charge and the person in charge of the treatment will apply measures

technical and organizational that are appropriate to the risk involved in 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 severity

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.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

8/16

IV

In this case, it is stated that the claimed entity provides details of the

last movements of the Affinity Card through a service system

automated telephone call on the telephone ***TELÉFONO.1 in which only

as identification data the client's ID.

Unless there is evidence to the contrary, these facts mean that the defendant would not adopt the

adequate security measures, since any person using the system of

Automated telephone service could give a DNI number whether or not you are the holder of the

same and obtain information associated with that DNI, since the claimed entity does not

adopts security measures to verify that the person requesting such

information is the holder of said identification document.

This Agency informed the entity of the claim filed and

requested information in relation to this claim, in accordance with the

article 65.4 of the RGPD.

On September 25, 2020, the entity claimed in response to said request

requests the stay of the procedure, in accordance with article 76.2 of the law

39/2015 of Common Administrative Procedure of Public Administrations,

alleging defects in the processing.

The Spanish Agency for Data Protection addressed the respondent, requiring

information in accordance with article 65.4 of the RGPD that establishes the following:

"Before deciding on the admission to processing of the claim, the Spanish Agency

of Data Protection may send it to the data protection delegate who

had, where appropriate, designated the person responsible or in charge of the treatment or the

oversight body established for the application of codes of conduct to

the effects foreseen in articles 37 and 38.2 of this organic law. The agency

Spanish Data Protection Authority may also send the claim to the

responsible or in charge of the treatment when a

data protection delegate or adhered to resolution mechanisms

out-of-court settlement of conflicts, in which case the person in charge or person in charge must give

response to the claim within a month."

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Said requirement is ex gratia, to discern the convenience or

not to admit the procedure for processing by virtue of the answer given by the

claimed to this Agency, to the extent possible to avoid initiating procedures

sanctioning when the situation object of the claim has already been solved or

there is a serious and verifiable purpose that is being solved, without detriment to

the investigative actions that the Spanish Agency for Data Protection,

as a control authority, it can always carry out, if it considers it opportune and

necessary, in accordance with article 57.1 of the RGPD.

Neither of the two is inferred from the response given by the respondent entity.

indicated possibilities.

Therefore, due to the facts claimed, that is, failure to adopt measures of

adequate security by the claimed entity, without respecting the principle of

integrity and confidentiality of article 5.1 f) of the RGPD, whose purpose, among others, is to avoid

unauthorized or illicit treatment of personal data, this Agency proceeds to

the opening of the corresponding sanctioning procedure against the entity

claimed, for the possible violation of article 32 of the RGPD, transcribed in the

foundation II that states that “the person in charge and the person in charge of the treatment will apply

appropriate technical and organizational measures to ensure a level of security

appropriate".

In addition, in accordance with article 32 of the RGPD, it will be required that the claimed

take appropriate technical and organizational measures to ensure a level of

adequate security using mechanisms that allow:

-pseudonymization and encryption of personal data;

-the ability to ensure confidentiality, integrity, availability and resiliency

permanent treatment systems and services;

-the ability to restore the availability and access to the personal data of

quickly in the event of a physical or technical incident;

-a process of regular verification, evaluation and assessment of the effectiveness of the

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

v

Article 83.4 a) of the RGPD establishes that:

Violations of the following provisions 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

of greater amount:

a) the obligations of the person in charge and of the person in charge pursuant to articles 8, 11, 25 a

39, 42 and 43

In turn, article 73.f) of the LOPDGDD, under the heading "Infringements considered

bass has:

“According to article 83.4 of Regulation (EU) 2016/679, they will be considered serious and

Infractions that suppose a substantial violation will prescribe after two years.

of the articles mentioned therein, and in particular the following:

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

appropriate to guarantee a level of security appropriate to the risk of the treatment,

in the terms required by article 32.1 of Regulation (EU) 2016/679.”

SAW

In accordance with the precepts indicated, against the infraction of article 32,

considers 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 the following:

 The number of clients of the defendant entity is high and therefore also the

number of affected (art. 83.2 a)

 The defendant is a solvent entity that has the technical means to take

adequate security measures, their lack supposes negligence in their actions

(article 83.2 b)

 The high degree of responsibility of the claimed party, since trying to

daily personal data of your customers as part of your business and

adopting appropriate security measures, including those of the

regulation for the prevention of fraud in banking entities, it is

fully aware of the need to implement security measures

appropriate to the risk in all the treatments you carry out, aggravates your

liability for lack of security measures (art. 83.2 d)

 Despite the previous requirements and attempts to communicate this Agency with the

entity claimed to know the situation from the point of view of all the

affected parties, the entity claimed, has not submitted allegations to the

prior requirement, rather than to request its suspension alleging errors in the

processing of a procedure not initiated, and without collaborating with this Agency in

their actions, despite being aware of the claim filed against

she (art. 83.2 f)

Therefore, based on the foregoing,

By the Director of the Spanish Data Protection Agency,

HE REMEMBERS:

FIRST: START SANCTION PROCEDURE against BANCO BILBAO

VIZCAYA ARGENTARIA, S.A., with NIF A48265169, in accordance with the provisions of

article 58.2.b) of the RGPD, for the alleged infringement of article 32 of the RGPD,

typified in article 83.4.a) of the RGPD.

SECOND: APPOINT instructor to B.B.B. and, as Secretary to C.C.C., indicating that

any of them may be challenged, where appropriate, in accordance with the provisions of the

Articles 23 and 24 of Law 40/2015, of October 1, on the Legal Regime of the Sector

Public (LRJSP).

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

claim filed by the claimant and his documentation, the documents

obtained and generated by the General Subdirectorate for Data Inspection during the

investigation phase, as well as the report of previous Inspection actions.

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

October and article 58.2.b) of the RGPD, it would be appropriate to impose a penalty of 200,000

euros (two hundred thousand euros) for the infringement of article 32 of the RGPD, without prejudice

of what results from the instruction.

FIFTH: NOTIFY this agreement to BANCO BILBAO VIZCAYA

ARGENTARIA, S.A., with NIF A48265169, granting it 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, in the event that the sanction to be imposed was a fine, it may recognize its responsibility within the term granted for the formulation of allegations to this initial agreement; it which will entail a reduction of 20% of the sanction to be imposed in the present procedure. With the application of this reduction, the sanction would be established at €160,000 (one hundred and sixty thousand euros), 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 €160,000 (one hundred and sixty thousand euros), 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 set at €120,000 (one hundred and twenty thousand euros).

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 €160,000 (one hundred and sixty thousand euros) or €120,000 (one hundred

twenty thousand euros), you must make it effective by depositing it in account number ES00

0000 0000 0000 0000 0000 opened in the name of the Spanish Agency for the Protection of

Data in the banking entity CAIXABANK, S.A., indicating in the concept the number

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

the reason for the reduction of the amount to which it avails itself.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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

>>

SECOND: On August 18, 2021, the claimed party has proceeded to pay

of the sanction in the amount of 120,000 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

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

control, and as established in art. 47 of the Organic Law 3/2018, of 5

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

hereinafter LOPDGDD), the Director of the Spanish Agency for Data Protection

is competent to sanction the infractions that are committed against said

Regulation; infractions of article 48 of Law 9/2014, of May 9, General

Telecommunications (hereinafter LGT), in accordance with the provisions of the

article 84.3 of the LGT, and the infractions typified in articles 38.3 c), d) and i) and

38.4 d), g) and h) of Law 34/2002, of July 11, on services of the society of the

information and electronic commerce (hereinafter LSSI), as provided in article

43.1 of said Law.

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."

In accordance with the above, the Director of the Spanish Agency for the Protection of

Data

RESOLVES:

FIRST: TO DECLARE the termination of procedure PS/00362/2021, 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.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

16/16

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

936-160721

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es