 File No.: PS/00375/2022

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 claimant) dated May 31, 2021

filed a claim with the Spanish Data Protection Agency. The

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

A48265169 (hereinafter, the claimed party or BBVA). The reasons on which the

claim are as follows:

On November 25, 2020, in his capacity as lawyer for Ms. B.B.B.,

filed a claim document with the BBVA entity on its behalf.

Subsequently, on December 1, 2020, the respondent entity delivered in

hand to his client, Ms. B.B.B., a letter relating to the claim addressed by BBVA

to the complaining party in which the private address of the latter is recorded, instead of the

corresponding to his professional office, violating the duty of confidentiality

of data (the complaining party is also a client of the entity). The complaining party

warns that BBVA has revealed his private address, which was not known to Ms.

B.B.B., which was provided to the entity due to its status as its client, with

occasion of opening a bank account. It also adds that it presented

claim before BBVA requesting compensation for these events and received

answer on December 31, 2020.

Provides the initial claim presented as a lawyer, which does not indicate

no contact postal address, and a copy of the email by which

sends the same to the claimed entity, dated 11/25/2020; BBVA's response

indicating to the claiming party the reference number assigned to the claim,

addressed to the claimant at his private address; WhatsApp screenshot by

that Mrs. B.B.B. sends said response to the complaining party; and writing from BBVA

responding to the second claim made for the incident that occurred with their

data, in which the entity apologizes and indicates that they have put the facts in

knowledge of those responsible involved in order to be able to adopt, in their

case, the appropriate measures.

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

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

forward LOPDGDD), said claim was transferred to the claimed party, for

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 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 06/22/2021 as stated in the

acknowledgment of receipt in the file.

On 09/01/2021, this Agency received a written response from BBVA

indicating that the response issued by the entity to acknowledge receipt of the claim

submitted by the complaining party on behalf of its client, which did not indicate

no address for communication purposes, it was sent to the only address

known by BBVA, which was included in the client database.

In addition, BBVA states that on December 1, 2020, Ms. B.B.B. he appeared in

the office of the entity requesting to know the status of your claim and a copy of the

proceedings. At that time, the Director of the office gave said person a

copy of the only document that existed to date, corresponding to the acknowledgment of

receipt of the claim.

Subsequently, on December 3, 2020, the claiming party submitted in another

BBVA office a new claim document on behalf of your client in which

indicated his professional address as address for the purposes of notifications.

On December 25, 2020, the SAC responded to the claim submitted, sending

said reply to the address indicated by the complaining party in its brief dated 3

December 2020, that is, your professional address.

THIRD: On October 6, 2021, in accordance with article 65 of the

LOPDGDD, the claim presented by the claimant party was admitted for processing.

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:

1. The claimed entity is a Spanish public limited company. According to

the data in “Axesor” refers to a large group parent company (…). No

files from before the present have been found in Sigrid in relation to

security breaches of this entity.

2. Information and documentation was requested from the requested entity and, from the response

received, the following follows:

a) Regarding the chronology of the events. Actions taken in order to

minimize the adverse effects and measures adopted for their final resolution.

On December 1, 2020, a client of the claiming party requests

copy of the claim that it filed on its behalf before BBVA. The

The respondent entity delivered by hand to this person the document related to the

claim, in the name of the claimant and in which the private address is stated

this.

BBVA, on December 23, 2020, responded to the claim of the claimant

apologizing for what happened, noting that said incident has been put into

knowledge of those responsible involved who have adopted measures to avoid

similar incidents.

Knowing the incidence by BBVA, the facts have been analyzed and verified that said

incident occurred due to a specific error, which was repaired immediately

Inform the complaining party of the address of his professional office.

BBVA clarifies that providing the person represented by the claimant with the

acknowledgment of receipt of the claim, without hiding the private address of the claim (address

used by the SAC as the address of the professional firm did not appear in the document),

It was a specific and isolated error.

b) Regarding the causes that made the gap possible

The person represented by the claimant requested the BBVA branch, on

December 2020, a copy of the claim file submitted by your

representative, since at that time the issue had not yet been resolved.

claim and only included the acknowledgment of receipt of the claim, this document will

was delivered by the Director of the office in which the address of the

domicile of the complaining party.

c) Regarding the affected data

The data affected was the private address of the claimant.

d) Regarding the security measures implemented

BBVA defends that: (i) it is a specific and involuntary error, since the Director

of the office was unaware that it was a private address and therefore a

personal data of the representative; (ii) that it was corrected, thus it is proven that

immediately adopted measures so that it did not happen again, using

mechanisms to reverse the situation and eliminate any risk of recidivism without

specify or certify them.

FIFTH: On 08/10/2022, the Director of the Spanish Agency for the Protection of

Datos agreed to initiate a sanctioning procedure against the entity BBVA, in accordance with the

provided in articles 63 and 64 of the LPACAP, for the alleged infractions

following:

. Violation of article 5.1.b) of the GDPR, typified in article 83.5.a) of the same

Regulation, and classified as very serious for the purposes of prescription in article

72.1.a) of the LOPDGDD.

. Violation of article 32 of the GDPR, typified in article 83.4.a) of the same

Regulation, and classified as serious for the purposes of prescription in article 73.f) and g)

of the LOPDGDD.

. Violation of article 5.1.f) of the GDPR, typified in article 83.5.a) of the same

Regulation, and classified as very serious for the purposes of prescription in article

72.1.a) of the LOPDGDD.

In the opening agreement it was determined that the sanction that could correspond,

attention to the existing evidence at the time of opening and without prejudice to the

resulting from the instruction, would amount to a total of 70,000 euros (seventy thousand

euros): 25,000 euros (twenty-five thousand euros) for the alleged infringement of article

5.1.b) of the GDPR, of 20,000 euros (twenty thousand euros) for the alleged infringement of the

Article 32 of the GDPR and 25,000 euros (twenty-five thousand euros) for the alleged

violation of article 5.1.f) of the GDPR.

Likewise, it was warned that the imputed infractions, if confirmed, may

lead to the imposition of measures in accordance with the provisions of the aforementioned article

58.2 d) of the GDPR.

SIXTH: The notification to the claimed party of the opening agreement outlined in the

previous antecedent, in which a term was granted to formulate allegations and

proposing evidence, it was sent through the Electronic Notification Service, and it was

delivered to BBVA on 08/11/2022.

SEVENTH: Notification of the aforementioned initiation agreement in accordance with the established regulations

in the LPACAP and after the period granted for the formulation of allegations, the

has verified that no allegation has been received 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 infractions of the RGPD attributed to the defendant and the sanctions that

they could prevail. 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

1. The complaining party is a private client of BBVA, as the holder of an account

banking. For this reason, he provided the aforementioned entity with his personal data, including the

relative to the postal address corresponding to your home address.

2. On 11/25/2020, in his capacity as lawyer, the claimant filed

before BBVA a claim on behalf of one of its clients.

3. On the same date of 11/25/2020, BBVA acknowledged receipt of the reported claim

in the Second Proven Fact by writing to the claimant and his

personal address, the one associated with your private client file as holder of a

bank account opened in this bank. Through this letter, BBVA informed the

complaining party the reference number assigned to the claim.

4. On 12/01/2020, BBVA provided the person represented by the party

claimant the document acknowledging receipt of the claim outlined in the Fact

Tested Third, revealing the data relating to the personal address of the

complaining party.

FUNDAMENTALS OF LAW

Yo

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

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

Control Authority, and as established in articles 47, 48.1, 64.2 and 68.1 of the

LOPDGDD, the Director of the Spanish Data Protection Agency is

competent to initiate and resolve this procedure.

Article 63.2 of the LOPDGDD determines that: "The procedures processed by the

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

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

In this case, the following facts are revealed, without any of them

they are controversial:

The claimant is a private client of BBVA, as the holder of an account

banking. For this reason, he provided the aforementioned entity with his personal data, including the

relative to the postal address corresponding to your home address.

In his capacity as lawyer and acting on behalf of and on behalf of one of his

customers, the claimant filed a claim with BBVA, of which this

entity acknowledged receipt by writing to the complaining party and his address

personal, the one associated with your particular client file as an account holder

Bank opened in this Bank.

In addition, BBVA provided the person represented by the claimant with this

document acknowledging receipt of the claim made, making it clear

the data relating to the personal address of the complaining party, which was not known by

this third person.

II

The facts exposed, in relation to the use of the personal data of the party

claimant relative to his private address for the processing of a claim

formulated by the same in name and representation of a third party, acting under its

lawyer status, without there being legitimate cause for it, suppose a

breach of the principle of "limitation of purpose" regulated in article 5.1.b)

of the GDPR, which establishes the following:

"1. Personal data will be:

(…)

b) collected for specific, explicit and legitimate purposes, and will not be further processed

in a manner incompatible with said purposes; according to article 89, paragraph 1, the

further processing of personal data for purposes of archiving in the public interest, purposes of

scientific and historical research or statistical purposes shall not be considered incompatible with the

initial purposes (“purpose limitation”).

In relation to the principles regulated in the aforementioned article 5 of the GDPR, it is taken into account

Consider what is stated in Recital 39 of the aforementioned GDPR:

“39. All processing of personal data must be lawful and fair. For natural persons, it must
make it completely clear that they are collecting, using, consulting or otherwise dealing with
way personal data concerning them, as well as the extent to which such data is or
they will be treated. The principle of transparency requires that all information and communication
regarding the processing of said data is easily accessible and easy to understand, and that it is
use simple and clear language. This principle refers in particular to the information of
the interested parties on the identity of the person responsible for the treatment and the purposes of the same and to the
added information to guarantee a fair and transparent treatment with respect to the
natural persons affected and their right to obtain confirmation and communication of the data
personal data concerning them that are subject to treatment. Natural persons must
be aware of the risks, standards, safeguards and rights relating to the
processing of personal data, as well as how to enforce your rights in relation to
with the treatment. In particular, the specific purposes of the processing of personal data
they must be explicit and legitimate, and must be determined at the time of collection. The
personal data must be adequate, relevant and limited to what is necessary for the purposes
for those who are treated. This requires, in particular, ensuring that it is limited to a minimum
its conservation period is strict. Personal data should only be processed if the purpose of the
treatment could not reasonably be accomplished by other means. To ensure that the
personal data is not kept longer than necessary, the data controller has
to establish deadlines for its suppression or periodic review. All measures must be taken
reasonable to ensure that any personal data that is
inaccurate. Personal data must be processed in a way that guarantees security and
appropriate confidentiality of personal data, including to prevent unauthorized access or use
authorized of said data and the equipment used in the treatment”.

In this case, BBVA processed personal data on the part
claimant incompatible with the purposes that determined the collection of such

data.

Consequently, the aforementioned facts violate the provisions of article 5.1.b) of the

GDPR, giving rise to the application of the corrective powers that article 58 of the

Said Regulation grants the Spanish Data Protection Agency.

IV.

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, the

scope, context and purposes of processing, as well as probability and severity risks

Variables for the rights and freedoms of natural persons, the person in charge and the person in charge

of the treatment will apply appropriate technical and organizational measures to guarantee a level

of security appropriate to the risk, which, where appropriate, includes, among others:

a) the pseudonymization and encryption of personal data;

b) the ability to ensure confidentiality, integrity, availability and resilience

permanent treatment systems and services;

c) the ability to restore the availability and access to personal data in a manner

fast in case of physical or technical incident;

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

technical and organizational to guarantee the security of the treatment.

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

risks presented by data processing, in particular as a result of the

destruction, loss or accidental or unlawful alteration of personal data transmitted,

stored or otherwise processed, or unauthorized communication or access to such

data.

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

certification approved under article 42 may serve as an element to demonstrate the

compliance with the requirements established in section 1 of this 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 having 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 GDPR defines breaches of personal data security as "all

those security violations that cause the destruction, loss or

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

otherwise, or unauthorized disclosure of or access to such data."

It should be noted that the GDPR does not establish a list of security measures

that are applicable according to the data that are processed, but

which 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 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 the provisions of the

this Regulation, the controller or processor must assess the risks inherent in the

treatment and apply measures to mitigate them, such as encryption. These measures should ensure

an appropriate level of security, including confidentiality, taking into account the state of

the technique and cost of its application with respect to the risks and the nature of the data

personnel that must be protected. When assessing the risk in relation to the safety of the

data, the risks deriving from data processing must be taken into account

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

transmitted, stored or otherwise processed, or unauthorized communication or access

to said data, susceptible in particular to cause physical, material or

immaterial".

In accordance with what is stated in Recital 74 of the GDPR, the person responsible for the

treatment corresponds to be able to demonstrate that the measures adopted are effective:

"The responsibility of the data controller must be established for any

processing of personal data carried out by himself or on his behalf. In particular, the

responsible must be obliged to apply timely and effective measures and must be able to

demonstrate the compliance of processing activities with this Regulation,

including the effectiveness of the measures. Such measures should take into account the nature,

scope, context and purposes of processing as well as the risk to rights and freedoms

of natural persons".

These technical and organizational measures are included as part of the principle of

active responsibility, which requires a prior assessment by the person responsible for the

treatment of the risk that the processing of personal data could generate,

from which the appropriate measures will be adopted.

With the GDPR, anticipation of the infringement or injury of rights is sought to

avoid it. This proactive focus on the "permanent implementation" of security measures

security implies that they are not static, but dynamic, corresponding

It is up to the data controller to determine at all times what are the measures of

necessary security measures to guarantee the confidentiality, integrity and

availability of personal data and mitigate or eliminate risks to

people rights. The first step is to carry out a "risk analysis" to

assess threats.

It is the person in charge or in charge of treatment who must prove said diligence

with a solid and effective internal control system. Therefore, the mere

formal demonstration of compliance, but this principle requires a prior attitude,

conscious, diligent and proactive on the part of the organizations in front of all the
processing of personal data that they carry out.

The mandatory nature of these measures, or the way in which they are applied, will depend on
factors that must be taken into account in each case, such as the type of treatment and the
risk that said treatment implies for the rights and freedoms of the interested parties.

Consequently, the due diligence must be adapted to the level of risks in the
protection of data and the characteristics of the organization.

The concept of due diligence can be defined as “the measure of prudence,
activity or assiduity that can be reasonably expected, and with which normally
acts, an organization prudently and reasonably in circumstances
determined; It is not measured by an absolute norm, but depending on the facts
relative to the case in question”. Therefore, due diligence is an ongoing process.
observation and prevention of the negative effects of the entities' activities
on data protection.

In the instant case, as shown by the facts, the defendant used the
personal data of the complaining party registered in their private client file
for the processing of a claim made by this claiming party in
third party name. In addition, he provided a third party with the acknowledgment document
of said claim, informing him of the personal data of the claiming party
relating to your home address.

This fact shows that the requested entity has not adopted in a
effective technical and organizational measures to ensure the safety
and confidentiality of the data of its clients, especially those aimed at preventing the
access to information by unauthorized third parties, as in fact occurred when the
The respondent entity itself provided the client of the complaining party with the document of

acknowledgment of receipt of the claim formulated, addressed to the claimant and his

personal address.

Consequently, the aforementioned facts violate the provisions of article 32 of the GDPR,

giving rise to the application of the corrective powers that article 58 of the aforementioned

Regulation grants the Spanish Data Protection Agency.

V

The aforementioned article 5 of the GDPR establishes the principles that must govern the

treatment of personal data and mentions, among them, that of "integrity and

confidentiality":

"1. Personal data will be:

(…)

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

including protection against unauthorized or unlawful processing and against its loss,

accidental destruction or damage, through the application of technical or organizational measures

appropriate ("integrity and confidentiality").

(…)".

The documentation in hand offers sufficient evidence to understand that the entity

claimed violated article 5 of the GDPR, which regulates the duty of confidentiality,

materialized in the disclosure to third parties of the personal data of the party

claimant, specifically, the one related to his private address. It is a diffusion

of personal data for which the requested party does not have a legal basis that

legitimate.

This duty of confidentiality is intended to prevent leaks from being made

of the data not consented by their owners.

Consequently, the aforementioned facts imply a violation of the provisions of the

Article 5.1 f) of the GDPR, which gives rise to the application of the corrective powers that the

Article 58 of the aforementioned Regulation grants the Spanish Agency for the Protection of

data.

SAW

BBVA, in its response to the process for forwarding the claim, has stated that

the facts verified took place due to a specific and isolated error, although not even

has explained what the alleged error consisted of.

In this regard, it is necessary to consider that the incidents that motivate the actions

occur within BBVA's area of responsibility and this entity must respond

thus. In no way can it be considered that the error that he claims to have committed

exclude its responsibility, since, according to settled jurisprudence, it cannot

The existence of such an error may be considered when it is attributable to the person who suffers it or could

be avoided by the use of increased diligence. In this case, the assumed error is

incompatible with the diligence that the claimed party is obliged to observe.

This diligence must be manifested in the specific case under analysis, in respect of which

the error is alleged, and not in general circumstances.

In the specific case of the complaining party, it cannot be accepted that the actions of the

claimed entity results from an error. Admitting that it is not appropriate to demand responsibility from

BBVA for the facts analyzed, based on an alleged error, would be as much as

admit that the application of the GDPR and the LOPDGDD can be ignored.

In this regard, it should be remembered that when the error shows a lack of

due diligence the rate is applicable. The National Court in the Judgment of 21

September 2004 (RCA 937/2003), pronounces itself in the following terms:

"In addition, as regards the application of the principle of guilt, it results (following the criterion of this Chamber in other Judgments such as the one dated January 21, 2004 issued in the appeal 1139/2001) that the commission of the offense provided for in article 44.3.d) can be both willful as guilty. And in this sense, if the error shows a lack of diligence, the guy is applicable…".

In this line it is worth mentioning the SAN of January 21, 2010, in which the Court exposes:

“The appellant also maintains that there is no guilt in her actions. Is true that the principle of guilt prevents the admission in administrative law sanctioning of strict liability, it is also true that the absence of intentionality is secondary since this type of infraction is normally committed due to negligent or negligent action, which is enough to integrate the subjective element of guilt. XXX's performance is clearly negligent because... he must know... the obligations imposed by the LOPD on all those who handle personal data of third parties. XXX is obliged to guarantee the fundamental right to the protection of personal data of its clients and hypothetical clients with the intensity required by the content of its own right".

The principle of guilt is required in the disciplinary procedure and thus the STC 246/1991 considers it inadmissible in the field of penalizing administrative law a responsibility without fault. But the fault principle does not imply that it can only

punish an intentional or voluntary action, and in this regard article 28

of Law 40/2015 on the Legal Regime of the Public Sector, under the rubric

"Responsibility" provides 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, unions and entities without legal personality and estates

independent or self-employed, who are responsible for them by way of fraud or

blame".

The facts set forth show that BBVA did not act with due diligence in

that she was obliged, that she acted with a lack of diligence. The Supreme Court (Sentences

of 04/16 and 22/1991) considers that from the guilty element it follows “...that the

action or omission, classified as an administratively sanctionable infraction, must be,

in any case, attributable to its author, due to intent or imprudence, negligence or ignorance

inexcusable". The same Court reasons that "it is not enough... for exculpation against

a typically unlawful behavior the invocation of the absence of guilt" but

that it is necessary to prove "that the diligence that was required by the person who

alleges its non-existence” (STS January 23, 1998).

Also connected to the degree of diligence that the data controller is

obliged to deploy in compliance with the obligations imposed by the

data protection regulations can be cited the SAN of 10/17/2007 (Rec. 63/2006),

which specified: "(...) the Supreme Court has been understanding that there is imprudence

whenever a legal duty of care is neglected, that is, when the offender does not

behaves with the required diligence”.

In addition, the National Court, in terms of data protection of

personal nature, has declared that "simple negligence or breach of

the duties that the Law imposes on the persons responsible for files or the

data processing to be extremely diligent..." (SAN 06/29/2001).

VII

In the event of an infringement of the provisions of the GDPR, among the

corrective powers available to the Spanish Data Protection Agency,

as supervisory authority, article 58.2 of said Regulation contemplates the

following:

"2 Each control authority will have all the following corrective powers indicated to

continuation:

(…)

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

processing operations have infringed the provisions of this Regulation;”

(...)

d) order the person in charge or in charge of the treatment that the treatment operations are

conform to the provisions of this Regulation, where appropriate, of a given

manner and within a specified period;

(…)

i) impose an administrative fine in accordance with article 83, in addition to or instead of the

measures mentioned in this section, according to the circumstances of each case

particular;".

According to the provisions of article 83.2 of the GDPR, the measure provided for in letter d)

above is compatible with the sanction consisting of an administrative fine.

VIII

Failure to comply with the provisions of article 5.1.b) and f) of the GDPR entails the commission of offenses typified in section 5.a) of article 83 of the GDPR, which under the heading "General conditions for the imposition of fines administrative" provides the following:

"5. Violations of the following provisions will be penalized, in accordance with the section 2, with administrative fines of a maximum of 20,000,000 EUR or, in the case of a company, of an amount equivalent to a maximum of 4% of the total annual turnover of the previous financial year, opting for the highest amount:

a) the basic principles for treatment, including the conditions for consent to tenor of articles 5, 6, 7 and 9".

On the other hand, the violation of article 32 of the GDPR is typified in the Article 83.4.a) of the aforementioned GDPR in the following terms:

"4. Violations of the following provisions will be penalized, in accordance with the paragraph 2, with administrative fines of a maximum of EUR 10,000,000 or, in the case of a company, of an amount equivalent to a maximum of 2% of the total annual turnover of the previous financial year, opting for the highest amount:

a) 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 establishes that "They constitute offenses 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".

For the purposes of the limitation period, article 72 of the LOPDGDD indicates:

“Article 72. Offenses considered very serious.

1. Based on what is established in article 83.5 of Regulation (EU) 2016/679, they are considered very serious and will prescribe after three years the infractions that suppose a violation substance 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 the Article 5 of Regulation (EU) 2016/679”.

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

"Based on what is established in article 83.4 of Regulation (EU) 2016/679, they are considered serious and will prescribe after two years the infractions that suppose a substantial infringement of the articles mentioned therein and, in particular, the following:

(…)

f) The lack of adoption of those technical and organizational measures that are appropriate to guarantee a level of security appropriate to the risk of the treatment, in the terms required by article 32.1 of Regulation (EU) 2016/679

g) The breach, as a consequence of the lack of due diligence, of the measures technical and organizational that had been implemented in accordance with the requirements of article 32.1 of Regulation (EU) 2016/679.

(…)”.

In this case, in accordance with the facts exposed, it is considered that the sanction that It would be appropriate to impose an administrative fine.

The fine imposed must be, in each individual case, effective, proportionate

and dissuasive, in accordance with the provisions of article 83.1 of the GDPR.

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

provisions of article 83, section 2, of the GDPR, which states the following:

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

individually, in addition to or in lieu of the measures contemplated in article 58,

section 2, letters a) to h) and j). When deciding to impose an administrative fine and its amount

in each individual case due account shall be taken of:

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

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

affected stakeholders and the level of damages they have suffered;

b) intentionality or negligence in the infraction;

c) any measure taken by the controller or processor to alleviate the

damages suffered by the interested parties;

d) the degree of responsibility of the controller or processor, taking into account

of the technical or organizational measures that have been applied by virtue of 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 if the

Controller or processor notified the infringement and, if so, to what extent;

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

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 certification mechanisms

approved under article 42, and

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

financial benefits obtained or losses avoided, directly or indirectly, through

the offence".

For its part, in relation to letter k) of article 83.2 of the GDPR, the LOPDGDD, in

its article 76, "Sanctions and corrective measures", establishes:

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

2016/679 will be applied taking into account the graduation criteria established in the

section 2 of said article.

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

may be taken into account:

a) The continuing nature of the offence.

b) Linking the offender's activity with data processing

personal.

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

infringement.

e) The existence of a merger process by absorption subsequent to the commission of the infraction,

that 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) Submission by the person responsible or in charge, on a voluntary basis, to

alternative conflict resolution mechanisms, in those cases in which there are

disputes between those and any interested party".

In accordance with the precepts indicated, for the purpose of setting the amount of the sanctions

to be imposed in the present case, it is considered appropriate to graduate them in accordance with

the following criteria established by the transcribed precepts:

In this case, the graduation criteria are considered concurrent as aggravating factors.

following:

. Article 83.2.b) of the GDPR: "b) intentionality or negligence in the infringement".

The negligence appreciated in the commission of the offense, considering that the

The defendant party used the personal data of the complaining party registered in

the entity in its capacity as a client, without taking into account that it intervened in the

made in the name and representation of a third party.

In this regard, what was declared in the Judgment of the Hearing

National of 10/17/2007 (rec. 63/2006) that, based on the fact that they are entities

whose activity involves continuous data processing, indicates that "...the

The Supreme Court has understood that there is imprudence whenever

disregards a legal duty of care, that is, when the offender does not

behave with the required diligence. And in the assessment of the degree of diligence has

to weigh especially the professionalism or not of the subject, and there is no doubt

that, in the case now examined, when the appellant's activity is

constant and abundant handling of personal data must be insisted on the

rigor and exquisite care to comply with the legal provisions in this regard".

It is an entity that processes personal data in a manner

systematic and continuous and that it must take extreme care in fulfilling its

data protection obligations.

This Agency understands that the diligence must be deduced from facts

conclusive, duly accredited and directly related

with the elements that make up the infringement, in such a way that it can be deduced

that it has occurred despite all the means provided by the

responsible to avoid it. In this case, the action of the claimed party does not

has this character.

. Article 76.2.b) of the LOPDGDD: "b) Linking the offender's activity

with the processing of personal data".

The high link between the activity of the offender and the performance of treatments

of personal data. The level of implementation of the entity and the

activity that it carries out, in which the personal data of millions of

of interested This circumstance determines a greater degree of demand and

professionalism and, consequently, the responsibility of the entity

claimed in relation to data processing.

. Article 83.2.k) of the GDPR: "k) any other aggravating or mitigating factor

applicable to the circumstances of the case, such as the financial benefits obtained

or losses avoided, directly or indirectly, through the breach".

. BBVA's status as a large company and volume of business. It consists in

the actions that said entity has (...).

The following circumstance is also considered to be mitigating:

. Article 83.2.a) of the GDPR: "a) the nature, seriousness and duration of the

infringement, taking into account the nature, scope or purpose of the operation

treatment in question as well as the number of interested parties affected and the

level of damages they have suffered".

The infringement is an anomaly that affects only the complaining party.

Considering the exposed factors, the value reached by the fines for the

imputed offenses is 25,000 euros (twenty-five thousand euros) for offenses

very serious (violation of articles 5.1.b) and 5.1.f) of the GDPR) and 20,000 euros

(twenty thousand euros) for a serious offense (violation of the provisions of article 32

of the GDPR).

IX

Once the infringements have been confirmed, it could be agreed to impose on the person in charge the adoption of

adequate measures to adjust its performance to the regulations mentioned in this

act, in accordance with the provisions of the aforementioned article 58.2 d) of the GDPR, according to the

which each control authority may "order the person responsible or in charge of the

processing that the processing operations comply with the provisions of the

this Regulation, where appropriate, in a certain way and within a certain

specified term…".

In such a case, this Agency could require the person in charge to adapt the

processing of personal data that it carries out in accordance with the data protection regulations

in accordance with what is indicated in the preceding Fundamentals of Law.

This case affects only the complaining party and has to do with the

improper use and communication of the personal data of the complaining party related to

his personal address, on the occasion of a claim in which he intervened under the

status of representative of the person concerned; and the entity BBVA has

stated that this circumstance was later corrected. Being so, it does not fit

in this case, urge the adoption of measures by the data controller.

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 BANCO BILBAO VIZCAYA ARGENTARIA, S.A., with NIF

A48265169, for a violation of article 5.1.b) of the GDPR, typified in article

83.5.a) of the same Regulation, and classified as very serious for the purposes of prescription

in article 72.1.a) of the LOPDGDD, a fine of 25,000 euros (twenty-five thousand

euro).

SECOND: IMPOSE BANCO BILBAO VIZCAYA ARGENTARIA, S.A., with NIF

A48265169, for a violation of article 32 of the GDPR, typified in article

83.4.a) of the same Regulation, and classified as serious for the purposes of prescription in the

article 73.f) and g) of the LOPDGDD, a fine of 20,000 euros (twenty thousand euros).

THIRD: IMPOSE BANCO BILBAO VIZCAYA ARGENTARIA, S.A., with NIF

A48265169, for a violation of article 5.1.f) of the GDPR, typified in article

83.5.a) of the same Regulation, and classified as very serious for the purposes of prescription

in article 72.1.a) of the LOPDGDD, a fine of 25,000 euros (twenty-five thousand

euro).

FOURTH: NOTIFY this resolution to BANCO BILBAO VIZCAYA

ARGENTARIA, S.A.

FIFTH: 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 term

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

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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