 File No.: PS/00206/2022

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 January 30, 2023, the Director of the Spanish Agency for

Data Protection agreed to initiate sanction proceedings against BANKINTER, S.A.

(hereinafter the claimed party). Once the initiation agreement has been notified and after analyzing the

allegations presented, on March 21, 2023, the proposal for

resolution which is transcribed below:

<<

File No.: PS/00206/2022

PROPOSED RESOLUTION OF SANCTION 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) filed a claim with the

Netherlands data protection authority. The claim is directed against

BANKINTER, S.A. with NIF A28157360 (hereinafter, BANKINTER). The reasons in

on which the claim is based are as follows:

The complaining party exercised its right of access before BANKINTER, receiving

response dated February 4, 2019 indicating that it does not appear in their records

as a client or ex-client.

Along with the claim, provide:

- Copy of an email from the complaining party to privacidad@bankinter.com,

dated January 29, 2019, in which you attach your request for access to your data

personal in PDF.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

- Copy of an email from privacidad@bankinter.com to the part

claimant, dated January 31, 2019, in which he was informed that the

transferred your request to the corresponding department, from which you will be given

response fulfilled within the time frame and manner established.

- Copy of an email from the complaining party to privacidad@bankinter.com,

dated February 12, 2019, in which it reports: "Good afternoon, Received your

response by mail today (attached), denying that he has any

product contracted with you, indicate that it is not true, since I have an account

open with you (***ACCOUNT.1). Attached document issued by you in

reference to this account. Therefore, please review your records again and proceed

with the request. All the best."

- Copy of an email from privacidad@bankinter.com to the complaining party,

dated February 14, 2019, in which you are informed: "We forwarded your request to the

corresponding department, from which you will be given a full response in the

term and manner established.

- Copy of a BANKINTER document, dated September 2017, addressed to the

complaining party, in which the information related to its operations with

Bankinter, necessary to complete your corresponding tax return

to the fiscal year of 2016, in which it appears that the complaining party is the account holder number ***ACCOUNT.1.

- Copy of a document signed by the claimant, dated January 29, 2019, in which he requests BANKINTER access to his personal data.

- Copy of a BANKINTER document, dated February 4, 2019, addressed to the complaining party, in which they are informed that they cannot attend to their request for access since your data does not appear in your records as a client or ex-client of the entity.

SECOND: Through the "Internal Market Information System" (hereinafter IMI), regulated by Regulation (EU) No. 1024/2012, of the European Parliament and of the Council, of October 25, 2012 (IMI Regulation), whose objective is to promote the cross-border administrative cooperation, mutual assistance between States members and the exchange of information, as of February 7, 2020, had input in this Spanish Data Protection Agency (AEPD) the aforementioned claim. He transfer of this claim to the AEPD is carried out in accordance with the provisions in article 56 of Regulation (EU) 2016/679, of the European Parliament and of the Council, of 04/27/2016, regarding the Protection of Physical Persons in what regarding the Processing of Personal Data and the Free Circulation of these Data (hereinafter, GDPR), taking into account its cross-border nature and that this Agency is competent to act as main control authority, given that BANKINTER has its registered office and sole establishment in Spain.

According to the information incorporated into the IMI System, in accordance with the established in article 60 of the GDPR, acts as a "control authority data subject", in addition to the Dutch data protection authority, the Portuguese authority. The latter under article 4.22 of the GDPR, given that the

Data subjects residing in this country are likely to be substantially

affected by the treatment object of this procedure.

THIRD: On July 3, 2020, in accordance with article 64.3 of the

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

guarantee of digital rights (LOPDGDD), the claim was admitted for processing

submitted by the complaining party.

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

of previous investigative actions to clarify the facts in

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

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

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

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

LOPDGDD, having knowledge of the following extremes:

In response to a request for information from this Agency, on April 30,

2020, BANKINTER representatives state that they have procedures

and adequate mechanisms to comply with the processing of the rights of

Data protection of the interested parties. They provide a copy of the procedure.

In relation to the reason why the response provided to the complaining party as

consequence of his exercise of the right of access in which there was no information

regarding the account ***ACCOUNT.1, the representatives of the entity indicate that they

there was a specific error in the application of the Rights Procedure. This made

said account is not located and identified as corresponding to the part

claimant, therefore Bankinter did not provide such information.

As of April 20, 2020, the error has been resolved, and an answer has been given

to the right of access of the complaining party in full. representatives

of the entity provide a copy of the email sent to the complaining party with the

information requested in an encrypted attached document, whose key is (...).

FIFTH: On April 25, 2022, the Director of the AEPD declared the expiration of

of the proceedings as more than twelve months have elapsed from the date of

admission to processing of the claim, new investigation actions were opened

with the number AI/00170/2020, and these new actions included the

documentation in E/02670/2020.

SIXTH: On June 28, 2022, from the Subdirectorate General of Inspection

of Data of this Agency a screenshot was taken on the website

https://monitoriza.axesor.es/, relative to the size and volume of business of the company

BANKINTER S.A., in which there is no information on the last financial year

filed (2021), but listed as a group parent company, with a

share capital of €269,659,846.

SEVENTH: On July 1, 2022, the Director of the AEPD adopted a project

decision to initiate disciplinary proceedings. Following the established process

in article 60 of the GDPR, on July 5, 2022 it was transmitted through the IMI system

this draft decision and the authorities concerned were informed that they had

four weeks from that time to raise pertinent objections and

motivated. The processing period for this disciplinary procedure was
automatically suspended during these four weeks, in accordance with the
provided in article 64.4 of the LOPDGDD.
Within the period for this purpose, the control authorities concerned did not present
pertinent and reasoned objections in this regard, therefore it is considered that all the
authorities agree with said draft decision and are bound by
this, in accordance with the provisions of paragraph 6 of article 60 of the GDPR.
This draft decision was notified to BANKINTER in accordance with the regulations
established in Law 39/2015, of October 1, on Administrative Procedure
Common Public Administrations (LPACAP) on July 11, 2022, as
It appears in the acknowledgment of receipt that is in the file.
EIGHTH: On January 30, 2023, the Director of the Spanish Agency for
Data Protection agreed to initiate sanction proceedings against BANKINTER, in order to
impose a fine of 1000 euros, in accordance with the provisions of articles 63 and 64
of Law 39/2015, of October 1, on the Common Administrative Procedure of
Public Administrations (hereinafter, LPACAP), for the alleged infringement of the
Article 15 of the GDPR, typified in Article 83.5 of the GDPR, in which it was indicated
He had a period of ten days to present allegations.
This start-up agreement, which was notified in accordance with the rules established in the
LPACAP by means of electronic notification, was not collected by BANKINTER within the
period of making available, understood as rejected in accordance with the provisions of the
art. 43.2 of the LPACAP dated February 12, 2023, as stated in the certificate
that works in the file.
NINTH: On February 24, 2023, BANKINTER filed a brief with
this Agency (request for a copy and sending a copy) in which you explain that you had
knowledge, through the Authorized Electronic Address (DEH), that the AEPD put

at the disposal of Bankinter S.A a notification with reference ***REFERENCE.1 and

matter "Opening Agreement" and that it is in a situation of

“Rejected”. But that, on this occasion, it had not been received by the AEPD

no notice communicating to Bankinter S.A, the provision of a notification

at the electronic headquarters Enabled electronic address (DEH) or at the Address

unique authorized electronic (DEHu), practice that is usual by the Agency.

Therefore, the reason for the rejection was due to the fact that Bankinter had not been aware of

that he had a notification in the Enabled Electronic Address. Therefore, he requested

that the aforementioned notification be sent again to Bankinter so that it could have

access to the content of the same and formulate the corresponding allegations and in its

case, propose the test that it deems pertinent.

On February 28, 2023, this Agency made Bankinter available to

through electronic means a copy of the initiation agreement of the present

sanctioning procedure, which was duly collected that same day, as

It appears in the acknowledgment of receipt that is in the file.

TENTH: On March 9, 2023, this Agency received, on time and

form, letter from BANKINTER in which it made allegations regarding the start-up agreement in the

which, in short, stated that BANKINTER had acted without intent or fault and that

the sanction was not proportionate since there were mitigating factors that had not been

taken into account and that the aggravating circumstances considered in the initiation agreement should not

be such. Requested that this disciplinary proceeding be archived or,

secondarily, that a warning be addressed to him or, failing that, that he be

a minimum fine.

ELEVENTH: A list of documents in hand is attached as an annex.

The procedure.

Of the actions carried out in this procedure and of the documentation

in the file, the following have been accredited:

PROVEN FACTS

FIRST: On January 29, 2019, the claimant sends an email to

privacidad@bankinter.com, in which you attach your request for access to your data

personal in PDF.

SECOND: On January 31, 2019, the claimant receives an email

from the address privacidad@bankinter.com, in which he is informed that the

transferred your request to the corresponding department, from which you will be given

response fulfilled within the time frame and manner established.

THIRD: On February 4, 2019, BANKINTER sent a document to the party

claimant, in which they are informed that they cannot attend to their request for access since

that your data does not appear in your records as a client or ex-client of the entity.

FOURTH: On February 12, 2019, the claimant sends an email to

privacidad@bankinter.com, in which he reports: "Good afternoon, Received your

response by mail today (attached), denying that he has any

product contracted with you, indicate that it is not true, since I have an account

open with you (***ACCOUNT.1). Attached document issued by you in

reference to this account. Therefore, please review your records again and proceed

with the request. All the best."

Along with this email, the claimant provides a copy of a document

of BANKINTER, dated September 2017, addressed to the complaining party, in the

that they are sent the information related to their operations with Bankinter, necessary

to complete your tax return for the year 2016,

in which it appears that the claimant is the owner of the account number ***ACCOUNT.1.

FIFTH: On February 14, 2019, the claimant receives an email

from privacidad@bankinter.com, in which he is informed: "We forward your request to

corresponding department, from which you will be given a full response in the

term and manner established.

SIXTH: On April 20, 2020, BANKINTER responded to the right of access of

the complaining party, by email sent to the complaining party with

your personal data by means of an encrypted attached document, whose key was (...).

FUNDAMENTALS OF LAW

Yo

Competence

In accordance with the powers that article 58.2 and 60 of Regulation (EU) 2016/679

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

control authority and as established in articles 47, 48.1, 64.2 and 68.1 of the

Organic Law 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 Protection Agency

of data.

Likewise, article 63.2 of the LOPDGDD determines that: "The procedures

processed by the Spanish Data Protection Agency will be governed by the provisions in Regulation (EU) 2016/679, in this organic law, by the provisions regulations dictated in its development and, insofar as they do not contradict them, with character subsidiary, by the general rules on administrative procedures."

II

previous questions

In the present case, in accordance with the provisions of article 4.1 of the GDPR, there is carrying out personal data processing, since BANKINTER carries out the collection and conservation of, among others, the following personal data of natural persons: name and surname, address and email, among others treatments.

BANKINTER carries out this activity in its capacity as data controller, given that it is the one who determines the ends and means of such activity, by virtue of article 4.7 of the GDPR. In addition, it is a cross-border treatment, since BANKINTER is established in Spain, although it provides services to other countries in the European Union.

The GDPR provides, in its article 56.1, for cases of cross-border processing, provided for in its article 4.23), in relation to the competence of the authority of main control, that, without prejudice to the provisions of article 55, the authority of control of the main establishment or of the only establishment of the person in charge or of the The person in charge of the treatment will be competent to act as control authority for the cross-border processing carried out by said controller or commissioned in accordance with the procedure established in article 60. In the case examined, as has been stated, BANKINTER has its only establishment in Spain, so the Spanish Agency for Data Protection is competent to act as the main supervisory authority.

For its part, the right of access to personal data is regulated in article 15

of the GDPR.

II

Allegations adduced

In relation to the allegations adduced to the agreement to initiate this

disciplinary procedure, we proceed to respond to them according to the order

exposed by BANKINTER:

1.- ABSENCE OF FAILURE AND FAULT IN BANKINTER'S ACTIONS

BANKINTER alleges that its response to the complaining party was due to an error

in consulting the requested information, which was only noticed when the AEPD

sent the information request to this entity.

And that the described incident –being clearly unfortunate– must be considered

as something punctual and isolated; something almost fortuitous that "escaped" the measures and resources

that Bankinter had for the management of the rights of the interested parties.

Indicates that:

(a) BANKINTER had and has appropriate technical and organizational measures

to respond to the rights of the interested parties under the strictest respect for the

GDPR, its principles and obligations. In particular, in reply to the

Requirement the Rights Procedure was provided as Document No. 1.

BANKINTER affirms that this procedure is reputedly effective. and not in vain

Bankinter is a financial institution that receives an average of more than 44 requests for

rights per month (reaching 83 requests in January and February 2023). However,

and even taking into account the huge number of requests that the entity has been

receiving and managing since 2018, only twelve have resulted in proceedings before

the AEPD. It is worth highlighting even more that, except for the case at hand, the rest have

ended either in the file of proceedings or in the inadmissibility of the claim for the

AEPD. These figures, in his opinion, do nothing more than show how

Bankinter's procedures and the entity's great diligence are robust.

In any case, he claims that

(b) Bankinter had and still has a specialized department that is in charge of

respond to all requests for rights of interested parties. have a

department that is in charge only of the answers to the rights

guarantees, in his opinion, that they are answered in a timely manner. Said department works

hand in hand with legal advice for those non-operative issues.

(c) Bankinter alleges that there is absolute traceability of the exercise of rights by

part of the stakeholders. All requests received through any

channel are managed through a computer program for this purpose and there is also

a procedure in place to ensure proper management of rights

exercised.

(d) It also indicates that all Bankinter employees have to take a course

of obligatory compliance in terms of data protection in which, among others and to

the effects of the case at hand, the importance of attending to

correctly and on time the requests for data protection rights.

In this regard, this Agency wishes to point out that it is not the subject of this procedure
evaluate the procedure that BANKINTER may have implemented for care
of the exercise of rights, but it is a matter of evaluating whether BANKINTER gave due
response to the request to exercise the right of access of the complaining party in
matter, in accordance with the provisions of the GDPR.

1.5. However, BANKINTER alleges that, as is the case, in general, with any
procedure; The measures and controls described, while robust, are not
infallible, being the event (we insist, isolated and punctual) occurred with the party
claimant, proof and consequence thereof.

1.6. In this regard, and as a complement to what has been indicated, it warns and emphasizes that the
procedures that Bankinter has in place to minimize the consequences of errors
that, as in the case at hand, can occur, presenting solutions
them quickly and efficiently. Thus, in the present case, even in full
COVID-19 pandemic, Bankinter, on April 20, 2020, responded and satisfied the
right of the complaining party as soon as he became aware of the situation after receiving
the AEPD Requirement.

In this regard, this Agency wishes to point out that responding to the request to exercise
right of access to the complaining party is nothing other than complying with the
provided by the GDPR.

1.7. A clearly isolated and punctual error (there is no better proof of this than the fact
that no claims have been resubmitted in this regard or indicating this
type of error) such as the one that occurred in the case at hand – which, no matter how much
protocol, review, manage and automate is impossible to avoid absolutely – no
must deny the adequate diligence that, in effect, Bankinter has before the exercise of
rights by the interested parties, which is measured and confirmed by their habitual behavior

and daily and by the existence of policies, controls and reaction capacity as the

above indicated.

In this regard, this Agency wishes to point out that the fact that there were no more

claims in this regard or "indicating this type of error" does not conclude a proof of

that it is "a clearly isolated and specific error", although it is not the subject of the

present proceeding evaluate more than if in the case of the complaining party

BANKINTER duly responded in a timely manner to the request to exercise

right of access in question.

1.8. BANKITER alleges that the adequate contextualization of the event that occurred with the

complaining party and its appreciation as an isolated error with respect to the

procedures and controls implemented by Bankinter is not a trivial matter,

since it allows disassociating such an event from culpable conduct on the part of

Bankinter, without which there can be no sanction.

1.9. In fact, as recognized by established jurisprudence, the principles

inspiring criminal order are applicable, with certain nuances, to the law

sanctioning administrative (for all, the Constitutional Court Judgment

–"STC"– no. 18/1981). The principle of guilt also applies in matters of

administrative offenses and their sanctioning regime as it is a

manifestation of the ius puniendi of the State. In this sense, it is inadmissible in

our legal system a regime of strict liability or without fault (STC

no. 76/1990).

In this regard, the art. 28.1 of Law 40/2015, of October 1, on the Legal Regime

of the Public Sector ("LRJSP"), expressly indicates that:

"Only may be penalized for acts constituting an administrative offense those

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

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

independent or autonomous patrimonies, which are responsible for them

title of fraud or guilt".

In other words, without proven intent or negligence, one cannot be responsible for an infraction.

1.10. BANKINTER alleges that it could perhaps be argued that it had to be negligent

because, otherwise, the mistake that in turn caused the error would not have been made.

inadequate attention to the right of the complaining party. However, understand that

argument should also be rejected as not acceptable in our law

sanctioning.

1.11. Indeed, a specific and extraordinary error (as has occurred in the case that

occupies) does not allow deducing by itself the existence of culpable behavior. It

would suppose the definitive objectification of guilt, where the result is equivalent to the element

subjective (structure proscribed in our sanctioning law –criminal or

administrative).

1.12. In these terms, the National Court has ruled repeatedly

sentences: an isolated error cannot give rise by itself to responsibility when

there is no fraud or guilt and the pertinent diligence has been acted upon. For all, the

Judgment of the National Court of December 23, 2013 (Rec. 341/2012) (which,

In addition, it is cited by the AEPD itself in numerous resolutions in which it applies

this doctrine –for example, the relapses in files E/05498/2017,

E/06654/2017 or E/00878/2018 –) determines in this regard that:

"The issue, therefore, must be resolved in accordance with the principles of law

punitive given that mere human error cannot give rise, by itself (and especially

especially when it occurs in isolation), to the attribution of consequences

sanctioning; because, to do so, it would incur a system of responsibility

objectively prohibited by our constitutional order.

In the field of protection of personal data, so that this error

may be relevant for punitive purposes, it must be a consequence -or be

made possible - by the absence of previous and adequate control procedures

aimed at its avoidance.

Only in this way will a factor of guilt appear in the company, assignable to the

imprudence (or "simple non-observance") due to the lack of articulation of protocols or

of security procedures. But these shortcomings must be investigated

and proof by the sanctioning administrative body (to which the burden rests

of its realization in destruction of the presumption of innocence).

(…)

Well, in the present case nothing of all this is said by the resolution

sanctioning, not serving either, for these purposes, the conclusion that, if

the error occurred, it is because the security protocols were not established or were

insufficient. This would be a false and conflicting conclusion with the fallible dimension

human.

It is not, then, a matter of guaranteeing the absence of errors through punitive law

but rather to articulate procedures to prevent them and also, later, to sanction if

Those protocols are not established or if they are insufficiently established"

In this regard, this Agency wishes to point out that this case is not an

punctual error or an isolated error, which in itself gives rise to liability without

there was fraud or fault on the part of BANKINTER.

Deny the concurrence of negligent action by BANKINTER

would be equivalent to acknowledging that his conduct -by action or omission- has been diligent.

Obviously, this perspective of the facts is not shared, since it has been

a proven lack of due diligence. A great company that performs

habitual processing of personal data of its clients, such as BANKINTER, must

exercise extreme care in fulfilling their obligations in terms of protection

of data, as established by jurisprudence. It is very illustrative, the SAN of 17

October 2007 (rec. 63/2006), assuming that these are entities whose

activity involves continuous processing of customer data, 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 due diligence. And in assessing the degree of diligence, consideration must be given

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 of constant and abundant

handling of personal data

must insist on the rigor and exquisite care

for complying with the legal provisions in this regard".

In the present case, the complaining party sent a first email on the 29th of

January 2019 requesting access to your personal data. BANKINTER replied

that he could not provide such data because he did not count as a client or ex-client of the

bank.

However, the complaining party sent a second email on February 12

of 2019 indicating to the bank that it was a customer and attached a series of

documentation proving such situation. And this second email doesn't

received a response from the bank.

In other words, the complaining party contacted the bank again so that it could

correct the response provided at first, but the bank did not give due

treatment of this request, not even once the complaining party provides the

corresponding documentation so that the bank could rectify such situation.

The fact that BANKINTER had not duly responded to the complaining party

once he contacts the bank again to get him out of his mistake on his first

response, itself proves the lack of due diligence that might be expected

of a bank of the category of BANKINTER, which continuously carries out processing

personal data of its customers.

1.13. BANKINTER alleges that the Agency itself has filed complaints based on

this fact, a specific error cannot be equivalent to a culpable behavior of the

that derives administrative responsibility. As an example, the file resolution of

proceedings of procedure E/06894/2020, where the AEPD acknowledges that:

"It is proven that the action of the defendant as the entity responsible for the

treatment, although it incurred in a breach of the provisions of the regulations of

data protection by including the address of the notified person, which was due to a

specific error, it has already implemented the necessary measures so that they do not return to

occurrence of the events that are the subject of this claim."

In this regard, this Agency wishes to point out that procedure E/06894/2020 deals with

of a substantially different assumption, since it is not even a question of a

exercise of rights but of an unauthorized dissemination of personal data. In

said procedure, it was decided to file the proceedings based on the fact that it was

of a specific error that was corrected as soon as it became known and that

Measures were put in place to prevent a similar situation from happening again.

both assumptions that do not occur in the present case since the bank did not give

due response to the complaining party as soon as it was informed that it was

client and they had to provide them with the data they had, nor has it been accredited

that the bank had taken steps to prevent a similar situation from occurring

repeat in the future.

1.14. In addition, BANKINTER alleges that as soon as it became aware of the error, it proceeded

to resolve it and to give access to the complaining party to the requested data, demonstrating

that it had adequate mechanisms to effectively resolve an incident

like the one that happened All this cannot be ignored by the AEPD when analyzing the

culpability (actually, its absence) of Bankinter in the case at hand.

In this regard, this Agency reiterates that BANKINTER was notified of its error by the

complaining party in his email dated February 12, 2019, in which

not only stated that he was a client, but also provided the relevant documentation

to prove such situation, and thus be able to obtain access to your data, as

I had previously requested, but this email was not duly answered. But

that access to the data of the complaining party was given once this Agency

required BANKINTER to provide information on this matter.

1.15. BANKINTER alleges that the AEPD itself has taken into account this type of circumstances in resolutions such as the one issued in file PS/00019/2021, in the that absence of guilt is appreciated as detailed below:

"In the present case, it is clear that the defendant once learned of the errors that were occurring in the data crossing with the Robinson list of Adigital, acted with due diligence, correcting the error detected by sending the dated 02/5/2020 a new list corrected to the one investigated and incorporating into its internal listing of the numbering object of the claim, henceforth ceasing the calls to the claimant. Consequently, it is not appreciated by the investigated the volitional element of guilt in the initially charged conduct."

In this regard, this Agency wishes to point out that procedure PS/00019/2021 deals with of a substantially different assumption, since it is not even a question of a exercise of rights but of making advertising calls once the exercised the right of opposition, nor is it an infringement of the GDPR but of the Law 9/2014, of May 9, General of Telecommunications. In this procedure, it decided to file the proceedings based on the fact that the error in the data crossing with the Adigital's Robinson listing was due to a specific error in the filtering system of numberings with the Robinson list of Adigital, there being no guilt in his behavior, since it was due to a change in the filtering system of Robinson numbers of Adigital during the period between the year 2020 and February 2021 beyond their control, since the one claimed, before knowing the incidence in the downloads of the Robinson list of Adigital, proceeded to correct diligently that error, as can be deduced from the chronology of the events and the content of the administrative file, reason for which the conduct initially

accused to the defendant lacks volitional element of guilt as it results as

consequence of someone else's error and consequently, the one now investigated lacks

responsibility for the facts initially charged.

However, in the present case, it is not an error resulting from someone else's change.

to the will of BANKINTER nor has BANKINTER acted with due

due diligence, having not given a due response to the request of the

complaining party not even when the latter had provided the information regarding

that he was a customer.

1.16. BANKINTER alleges that, in other proceedings, such as E/06746/2020, the

AEPD has archived the actions for having the denounced reasonable measures to

avoid errors and act diligently to update them when the entity becomes aware of

which were not enough:

"From the investigation actions it can be deduced that (...) it had measures

preventive technical and organizational measures in order to avoid this type of incident but, without

However, the incident now analyzed occurred.

(…)

the investigated entity had reasonable technical and organizational measures in place to

avoid this type of incidence and that, when they are insufficient, have been updated accordingly.

diligent manner."

In this regard, this Agency wishes to point out that procedure E/06746/2020 deals with

of a substantially different assumption, since it is not even a question of a

exercise of rights but a personal data breach. in said

procedure, it was decided to file the proceedings based on the fact that the entity

investigated had reasonable technical and organizational measures in place to avoid this

type of incident and which, as they are insufficient, have been updated regularly

diligent, which is not what has happened in the present case since the bank

acted with due diligence by not giving due response to the complaining party in

when he informed him that he was a client and they should provide him with the information that

they had, nor has it been proven that the bank had adopted measures

to prevent a similar situation from happening again in the future.

1.17. BANKINTER alleges that, since the inadequate attention to the right of access

of the complaining party was due to a specific error and not to a behavior

Bankinter's negligence, the AEPD must file this Procedure

Penalty for not concurring the element of guilt.

In this regard, this Agency reiterates that denying the concurrence of an action

negligence on the part of BANKINTER would be equivalent to recognizing that its conduct - for

act or omission - has been diligent. Obviously, this perspective is not shared

the facts, since the lack of due diligence has been proven. A great

company that routinely processes the personal data of its

customers, such as BANKINTER, must exercise extreme care in complying with their

data protection obligations, as established by jurisprudence.

The SAN of October 17, 2007 (rec. 63/2006) is very illustrative, based on

that these are entities whose activity entails the continuous treatment of

customer data, indicates that "...the Supreme Court has understood that there is

recklessness whenever a legal duty of care is neglected, that is, when the

offender does not behave with the required diligence. And in the assessment of the degree of

diligence, the professionalism or not of the subject must be specially considered, and not

there is no doubt that, in the case now examined, when the activity of the appellant

is of 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".

In the present case, the complaining party sent a first email on the 29th of

January 2019 requesting access to your personal data. BANKINTER replied

that he could not provide such data because he did not count as a client or ex-client of the

bank.

However, the complaining party sent a second email on February 12

of 2019 indicating to the bank that it was a customer and attached a series of

documentation proving such situation. And this second email doesn't

received a response from the bank.

In other words, the complaining party contacted the bank again so that it could

correct the response provided at first, but the bank did not give due

treatment of this request, not even once the complaining party provides the

corresponding documentation so that the bank could rectify such situation.

The fact that BANKINTER had not duly responded to the complaining party

once he contacts the bank again to get him out of his mistake on his first

response, itself proves the lack of due diligence that might be expected

of a bank of the category of BANKINTER, which continuously carries out processing

personal data of its customers.

For all of the foregoing, this claim is dismissed.

2. - SUBSIDIARILY, REGARDING THE NECESSARY PROPORTIONALITY OF THE SANCTIONS AND ITS GRADUATION. APPLICATION OF MITIGATION AND ABSENCE OF AGGRAVANTS.

2.1. Subsidiarily to the First Allegation, in the unlikely event that Bankinter is considered responsible for the infringement of article 15 when assessing some type of fault (quod non), BANKINTER alleges that the Agency must take into consideration of the following extenuating circumstances (which are ruled out in the Settlement Agreement Start without stopping to analyze them), in order to determine the amount of the fine and the imposition of the warning, in accordance with the provisions of arts. 83.2 GDPR and 76.2 of the LOPDGDD:

(a) The nature, seriousness and duration of the breach, taking into account the nature, scope or purpose of the processing operation in question such as the number of interested parties affected and the level of damages that have suffered (art. 83.2.a GDPR)

In the case at hand, the situation that occurred has implied a late response before the exercise of the right of access of a single person due to a specific error.

It can only be understood that the provisions of art. 83.2.a GDPR apply to this case as an extenuating circumstance.

In this regard, this Agency wishes to point out that it is not that BANKINTER had given a "late response" to the complaining party, but it is that the bank had not provided a response of any kind to the complaining party and was only provided with the access once the claim has been admitted for processing and after it has been required to provide information on the case.

According to the Ruling of the National Court SAN 3432/2009, "the lack of answering the access requests of the complainant and their delivery to another

company, configures the obstruction of the right of access that all affected

recognizes article 15 of the LOPD, and that article 44.3 e) classifies as an infraction

serious". That is to say, that the fact of not having provided access to the part

claimant to the data that BANKINTER had, it is an obstacle

of the right of access.

For this reason, it cannot be understood that such a situation is valued as a mitigation of

the infringement, but the opposite. Therefore, this claim is dismissed.

(b) The intentionality or negligence in the infringement (art. 83.2.b GDPR)

BANKINTER alleges that it has acted with due diligence, implementing measures

before and after a specific error, both preventively and proactively to guarantee the

protection of the personal data it processes, and to give a proper response to the

rights. And that in the rare event that the AEPD considers that there is fault, it has

It has been demonstrated that this circumstance must be understood as an attenuation.

In this regard, this Agency reiterates that denying the concurrence of an action

negligence on the part of BANKINTER would be equivalent to recognizing that its conduct - for

act or omission - has been diligent. Obviously, this perspective is not shared

the facts, since the lack of due diligence has been proven. A great

company that routinely processes the personal data of its

customers, such as BANKINTER, must exercise extreme care in complying with their

data protection obligations, as established by jurisprudence.

The SAN of October 17, 2007 (rec. 63/2006) is very illustrative, based on

that these are entities whose activity entails the continuous treatment of

customer data, indicates that "...the Supreme Court has understood that there is

recklessness whenever a legal duty of care is neglected, that is, when the

offender does not behave with the required diligence. And in the assessment of the degree of

diligence, the professionalism or not of the subject must be specially considered, and not

there is no doubt that, in the case now examined, when the activity of the appellant

is of 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".

In the present case, the complaining party sent a first email on the 29th of

January 2019 requesting access to your personal data. BANKINTER replied

that he could not provide such data because he did not count as a client or ex-client of the

bank.

However, the complaining party sent a second email on February 12

of 2019 indicating to the bank that it was a customer and attached a series of

documentation proving such situation. And this second email doesn't

received a response from the bank.

In other words, the complaining party contacted the bank again so that it could

correct the response provided at first, but the bank did not give due

treatment of this request, not even once the complaining party provides the

corresponding documentation so that the bank could rectify such situation.

The fact that BANKINTER had not duly responded to the complaining party

once he contacts the bank again to get him out of his mistake on his first

response, itself proves the lack of due diligence that might be expected

of a bank of the category of BANKINTER, which continuously carries out processing

personal data of its customers.

For all the foregoing, this claim is dismissed.

(c) Any measure taken by the controller or processor to

alleviate the damages suffered by the interested parties (art. 83.2.c GDPR)

BANKINTER alleges that when knowledge of the error in the response gave

response to the right of access of the complaining party without any

additional damages for the delay in answering. This should also be taken into

considered as an extenuating circumstance.

In this regard, this Agency reiterates that BANKINTER was notified of its error by the

complaining party in his email dated February 12, 2019, in which

not only stated that he was a client, but also provided the relevant documentation

to prove such situation, and thus be able to obtain access to your data, as

I had previously requested, but this email was not duly answered. But

that access to the data of the complaining party was given once this Agency

required BANKINTER to provide information on this matter. which, by

other hand, it was nothing other than his obligation.

Therefore, this claim is dismissed.

(d) The degree of cooperation with the supervisory authority in order to remedy

the infringement and mitigate the possible adverse effects of the infringement (art. 83.2.f GDPR)

In line with the aforementioned, BANKINTER alleges that it adopted the measures

necessary to remedy the situation that occurred, of which he duly informed

to said Agency in the response to the Request. Bankinter has collaborated

good faith with the AEPD to remedy the infringement and, in fact, it was achieved, it was

which should be taken into account as an extenuating circumstance.

In this regard, this Agency wishes to point out that answering the requirements of

information that you make is a legal obligation, by virtue of article 52 of the

LOPDGDD, which provides that: "Public Administrations, including tax

and Social Security, and individuals will be obliged to provide the

Spanish Agency for Data Protection the data, reports, background and

supporting documents necessary to carry out their research activity". Hence

it was BANKINTER's obligation to provide said information to this Agency.

For all the foregoing, this claim is dismissed.

2.2. BANKINTER alleges that this case should not involve the imposition

of a fine, but in any case the warning (faculty of the AEPD recognized in

the art. 58.2.b of the GDPR). This, in accordance with recital 148 GDPR, can

prevail based on:

"In the event of a minor offence, or if the fine likely to be imposed

constitutes a disproportionate burden on a natural person, rather than

penalty by means of a fine, a warning may be imposed. should however

special attention should be paid to the nature, seriousness and duration of the infringement, to its

intentional nature, to the measures taken to alleviate the damages suffered,

to the degree of responsibility or any relevant prior infringement, to the manner in which

that the supervisory authority has become aware of the infringement, to compliance

of measures ordered against the person in charge or in charge, to adherence to codes of

conduct and any other aggravating or mitigating circumstances."

It indicates that in the case that concerns us, there is no doubt that we are facing a minor offence, without the fact that it is classified as "very serious" for mere of prescription, may change such consideration.

In this regard, this Agency wishes to point out that the requirements indicated by the recital 148 of the GDPR, every time we are not facing a slight infringement of the effects of the GDPR, as it is an obstacle to the exercise of the right of access by the complaining party due to BANKINTER's lack of due diligence, nor Nor is it a sanction directed at a natural person. For what is rejected the present claim.

23. The absence of consideration of the mitigating factors mentioned, and of the consequent reduction of the proposed amount or the imposition of a warning, would render the amount currently proposed completely contrary to principle of proportionality that governs the sanctioning administrative procedure in relation to with the infraction in dispute, resulting in a disproportionate penalty (for small as it is).

In this regard, this Agency reiterates all of the above and dismisses the present allegation.

IV.

Right of access

Article 15 "Right of access of the interested party" of the GDPR establishes:

"1. The interested party shall have the right to obtain from the data controller confirmation of whether or not personal data concerning you is being processed and, in such case, right of access to personal data and the following information:

a) the purposes of the treatment;

b) the categories of personal data concerned;

c) the recipients or categories of recipients to whom they were communicated

o personal data will be communicated, in particular recipients in

third countries or international organizations;

d) if possible, the expected period of conservation of personal data or,

if not possible, the criteria used to determine this term;

e) the existence of the right to request from the controller the rectification or

deletion of personal data or limitation of data processing

personal information relating to the interested party, or to oppose said treatment;

f) the right to file a claim with a control authority;

g) when the personal data has not been obtained from the interested party, any

available information on its origin;

h) the existence of automated decisions, including the elaboration of

profiles, referred to in article 22, sections 1 and 4, and, at least in such

cases, significant information about the logic applied, as well as the

importance and the expected consequences of such processing for the

interested.

2. When personal data is transferred to a third country or to an organization

international, the interested party shall have the right to be informed of the guarantees

appropriate under Article 46 relating to the transfer.

3. The data controller shall provide a copy of the personal data object of

treatment. The person in charge may receive for any other copy requested by the
interested party a reasonable fee based on administrative costs. when the
The interested party submits the application by electronic means, and unless he requests
otherwise provided, the information will be provided in an electronic format of
Common use.
4. The right to obtain a copy mentioned in section 3 will not negatively affect
to the rights and liberties of others".
In the present case, it is clear that the complaining party had requested BANKINTER the
access to your personal data by email in at least two
occasions. The last time, on February 12, 2019, in which he put in
knowledge of the bank that it was a customer and provided the relevant documentation
to prove that point.
For its part, BANKINTER replied the first time that it did not have his data and the
second time only sent an email to the complaining party
indicating that your application had been forwarded to the department
corresponding, from which a full response would be given in the term and manner
established. However, the complaining party did not receive any subsequent response.
until, after receiving the information request from this Agency,
you were given access to the requested information on April 20, 2020. This is more than one
year after having requested it and only after the intervention of this Agency.
According to the evidence available at this time in
agreement on the proposed resolution of the disciplinary procedure, it is considered that
the known facts could constitute an infringement, attributable to
BANKINTER, for violation of article 15 of the GDPR.
Classification and classification of the offense
V

In accordance with the evidence available at the present time of

proposed resolution of the disciplinary procedure, it is considered that

BANKINTER has not duly attended to the right of access requested by the party

claimant.

The known facts could constitute an infringement, attributable to

BANKINTER, typified in Article 83.5 of the GDPR, which stipulates the following:

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

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

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

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

the highest amount:

(…)

b) the rights of the interested parties in accordance with articles 12 to 22; (…)"

For the purposes of the limitation period for infringements, the alleged infringement

prescribes after three years, in accordance with article 72.1.k) of the LOPDGDD, which qualifies as

the following behavior is very serious:

"[k) The impediment or the obstruction or the repeated non-attention of the exercise

of the rights established in articles 15 to 22 of Regulation (EU)

2016/679]."

SAW

Sanction proposal

This infraction can be sanctioned with a fine of a maximum of €20,000,000 or,

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

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

of greater amount, in accordance with article 83.5 of the GDPR.

Likewise, for the purposes of deciding on the imposition of an administrative fine and its

amount, in accordance with the evidence available in this

moment of proposal of resolution of disciplinary procedure, it is considered that

the balance of the circumstances contemplated in article 83.2 of the GDPR and 76.2 of

the LOPDGDD, with respect to the offense committed by violating what is established in the

Article 15 of the GDPR, allows you to propose a penalty of €1,000 (one thousand euros).

VII

adoption of measures

If the infringement is confirmed, it could be agreed to impose on the person responsible 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…". The imposition of this measure is compatible with the sanction

consisting of an administrative fine, according to the provisions of art. 83.2 of the GDPR.

It is noted that not attending to the possible order to adopt measures imposed by

this body in the sanctioning resolution may be considered as a

administrative offense in accordance with the provisions of the GDPR, classified as

infraction in its article 83.5 and 83.6, being able to motivate such conduct the opening of a

subsequent administrative sanctioning procedure.

In view of the foregoing, the following is issued

PROPOSED RESOLUTION

That the Director of the Spanish Agency for Data Protection sanctions

BANKINTER, S.A., with NIF A28157360, for a violation of Article 15 of the GDPR,

typified in Article 83.5 of the GDPR, with a fine of €1,000.00 (one thousand euros).

Likewise, in accordance with the provisions of article 85.2 of the LPACAP, you will be

informs that it may, at any time prior to the resolution of this

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

It will mean a reduction of 20% of the amount of the same. With the application of this

reduction, the sanction would be established at 800.00 euros and its payment will imply the

termination of the procedure, without prejudice to the imposition of the measures

corresponding. The effectiveness of this reduction will be conditioned by the

withdrawal or waiver of any administrative action or appeal against the

sanction.

In case you choose to proceed to the voluntary payment of the specified amount

above, in accordance with the provisions of the aforementioned article 85.2, you must do it

effective by entering the restricted account number IBAN: ES00-0000-0000-0000-

0000-0000 (BIC/SWIFT Code: CAIXESBBXXX) opened in the name of the Agency

Spanish Data Protection Agency at 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, for voluntary payment, of reduction of the

amount of the penalty. Likewise, you must send proof of income to the

Sub-Directorate General of Inspection to proceed to close the file.

By virtue of this, you are notified of the foregoing, and the procedure is revealed.

so that within TEN DAYS you can allege whatever you consider in your defense and

present the documents and information that it deems pertinent, in accordance with

Article 89.2 of the LPACAP.

B.B.B.

INSPECTOR - INSTRUCTOR

926-170223

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

21/22

EXHIBIT

>>

SECOND: On March 28, 2023, the claimed party has proceeded to pay

of the sanction in the amount of 800 euros making use of the reduction provided for in the

motion for a resolution transcribed above.

THIRD: The payment made entails the waiver of any action or resource in the

against the sanction, in relation to the facts referred to in the

resolution proposal.

FUNDAMENTALS OF LAW

Yo

Competence

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

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

control authority and as established in articles 47, 48.1, 64.2 and 68.1 of the

Organic Law 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 Protection Agency

of data.

Likewise, article 63.2 of the LOPDGDD determines that: "The procedures

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

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

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

subsidiary, by the general rules on administrative procedures."

II

Termination of the procedure

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

Common for Public Administrations (hereinafter LPACAP), under the heading

"Termination in disciplinary proceedings" provides the following:

"1. Initiated a disciplinary procedure, if the offender acknowledges his responsibility,

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

2. When the sanction has only a pecuniary 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 presumed perpetrator, in

any moment 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 offence.

3. In both cases, when the sanction is solely pecuniary in nature, the
The competent body to resolve the procedure will apply reductions of at least
20% of the amount of the proposed penalty, these being cumulative among themselves.
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 resource against the sanction.
The percentage reduction provided for in this section may be increased
according to regulations."

According to what has been stated,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: DECLARE the termination of procedure PS/00206/2022, in
in accordance with the provisions of article 85 of the LPACAP.

SECOND: NOTIFY this resolution to BANKINTER, S.A..

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 as prescribed by
the art. 114.1.c) of Law 39/2015, of October 1, on Administrative Procedure
Common of Public Administrations, interested parties may file an appeal
administrative litigation before the Administrative Litigation 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.

Mar Spain Marti

Director of the Spanish Data Protection Agency

968-171022

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es