 File No.: EXP202104875

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 February 1, 2022, 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 September 8, 2022 the proposal was issued

resolution that is transcribed below:

<<

File no.: EXP202104875

PROPOSED RESOLUTION OF SANCTION PROCEDURE

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

to the following:

BACKGROUND

FIRST: D.A.A.A. (hereinafter, the claimant) dated 10/08/2021

filed a claim with the Spanish Data Protection Agency. The

claim is directed against BANKINTER, S.A. with NIF A28157360 (hereinafter, the

claimed party). The reasons on which the claim is based are the following:

access your personal area on the website of the claimed entity, in the section

corresponding to the monthly statement, not only the movements of your account are included, but also

also the movements of another belonging to a third party. As a consequence of

For this, on 07/16/2021 he files a claim with the Customer Service of

said entity and receives a response on 07/22/2021, reporting the start of the

timely actions without having received any further news in this regard, in addition to not

the incident has been corrected.

Provide a printout of the "monthly statement" document that appears in the personal area of the

claimant, corresponding to the month of June 2017, as well as the claim e-mail

and answer offered.

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.



No response to this letter has been received.

THIRD: On 12/29/2021 [the Director of the Spanish Protection Agency

de Datos agreed to admit the claim presented by the claimant for processing.

FOURTH: On 02/01/2022, the Director of the Spanish Protection Agency

of Data agreed to start a sanctioning procedure against the person claimed by the alleged

violation of articles 5.1.f) and 32.1 of the GDPR, typified in articles 83.5.a) and

83.4.a) of the aforementioned Regulation.

FIFTH: Notified of the initiation agreement, the defendant requested the extension on 02/09/2022

the deadline to answer and 02/14/2022 copy of the file; expansion that was

granted and copy that was transferred to him on 02/11/2022 and 02/14/2022 respectively.

The defendant submitted a brief of allegations on 02/25/2022 stating, in summary:

that it is not true, as stated in the initiation agreement, that it did not respond to the

requirements of the AEPD, since the response occurred on 12/27/2021; that

the incident was caused by an error when managing the change of ownership

of the other account of which in the past he was a co-owner, not updating correctly

the information that appeared in the claimant's "monthly statement" document,

to exclude that relating to the other account; the absence of fraud and guilt in the

action of the defendant; the non-existence of infringement of article 32.1 of the GDPR to the

have the claimed implemented appropriate technical and organizational measures; the

existence of medial contest of infractions; disproportionate sanctions

proposals and the necessary applications of mitigating factors and the absence of aggravating factors; he

filing of the procedure and subsidiarily the reduction of sanctions

proposals.

SIXTH: On 03/29/2022, the procedure instructor agreed to open

a period of practice tests, agreeing on the following:

- Consider reproduced for evidentiary purposes the claims filed by

the claimants and their documentation, the documents obtained and generated

by the Inspection Services that are part of the file.

- Consider reproduced for evidentiary purposes, the allegations to the agreement of

beginning presented by the defendant and the documentation that accompanies it.

SEVENTH: Of the actions carried out in this procedure, have been

accredited the following proven facts:

1. On 10/08/2021, a written entry from the claimant was entered in the AEPD stating that at

access the website of the defendant, personal area section corresponding to extract

monthly, not only the movements of your account are shown, but also the movements

from another account belonging to a third party; complaint filed with the Service of

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es



Customer Service received a response informing them of the start of the proceedings

opportune, without having received further news in this regard, in addition to not having

corrected the incident.

2. There is a copy of the claimant's DNI.

3. There is a copy of the integral monthly extract of June 2021 related to the

movements of account no. ***ACCOUNT.1 of which the claimant is the owner, as well as

of the movements of the account ***ACCOUNT.2 whose owner is a third person.

4. There is an email sent by the claimant to the claimant dated

07/16/2021, which states the following:

“Yesterday, Thursday, July 15, I accessed my personal account on the website of

Bankinter in order to check a payment made last month. Was

reviewing the movements of my account when, what is my surprise to discover that

The movements of another account of which I am not the owner also appear. that other

account, as shown. corresponds to a "gold pension current account".

(…)

In accordance with the foregoing, I request that you proceed to the immediate correction of this

situation.

(…)”

5. There is a response to the email, dated 07/22/2021, stating:

"Dear Customer:

We proceed to carry out the appropriate steps based on the situation raised”.

6. The defendant has provided a letter sent to the claimant dated 08/19/2021 in the

which indicates the following:

"Regarding the situation raised by you, we inform you that we have

transferred your comments to the commercial managers of your accounts to discuss

this issue.

Thanking you as always for the trust you have placed in Bankinter, we continue to

available through Telephone Banking, at bankinter.com or at any point of

our Commercial Network.

Likewise, we know that they have tried to reach him several times by phone without

success.

For any questions regarding the claim, you can call us at the Customer Service

Customer Service (Tel. 900 802 081), providing us with the reference number”.

7. The defendant in writing dated 02/25/2022 has stated that: "Actually, the

situation was caused by an error when managing the change of ownership of

the Other Account (as the Claimant himself stated in the Brief). I don't know

had completely withdrawn access to the information of the Other Account (of which

he had been co-owner) when the change of ownership occurred, to the extent

in which the information that appeared in the document was not updated correctly

"monthly statement" of the Claimant, to exclude that relating to the Other Account".



FUNDAMENTALS OF LAW

By virtue of the powers that article 58.2 of the GDPR recognizes to each control authority, and as established in articles 47 and 48 of the LOPDGDD, the Director of the Spanish Data Protection Agency is competent to initiate and to solve this procedure.

Yo

Likewise, article 63.2 of the LOPDGDD determines that:

"The procedures processed by the Spanish Data Protection Agency will be governed by the provisions of Regulation (EU) 2016/679, in this organic law, for the regulatory provisions dictated in its development and, as soon as they are not contradict, on a subsidiary basis, by the general rules on the administrative procedures."

II

The denounced facts materialize in the visualization, when accessing the monthly statement of your account on the claimant's website, not just your data personal but to the data of a third person (account number and movements of the same), violating the duty of confidentiality motivated by an incident of security due to breach of technical and organizational measures.

Article 58 of the GDPR, Powers, states:

"2. Each supervisory authority shall have all the following powers corrections listed below:

(…)

b) sanction any controller or processor with warning when the processing operations have infringed the provided in this Regulation;

(…)"

First of all, article 5, Principles relating to treatment, of the GDPR

states that:

"1. Personal data will be:

(…)

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

personal data, including protection against unauthorized processing or

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

of appropriate technical or organizational measures ("integrity and

confidentiality").

(…)"



II

1. First, the defendant in writing 02/25/2022 alleged that the

12/27/2021, through the Agency's electronic headquarters, responded to the

Transfers of Claim and Request for Information, as reflected in those in the

File itself containing a copy of the response offered and that in the

Initiation Agreement, it is indicated that no response has been received to the Transfers of

Claim and Information Request.

Obviously it is an error because the defendant is true that he answered, such

and as stated in the file, although such circumstance is contrary to what is alleged by

the defendant would not have implied the inadmissibility of the claim or non-compliance

of the norms that regulate the procedure in light of the information offered by the

same.

Secondly, in a brief of 04/07/2022, it alleged that the defendant did not

There was no record or procedure with the AEPD that corresponds to the

reference numbers (PS/00634/2021 or E/12527/2021) and requested confirmation of the

existence of said error and, in particular, that the reference to "the documents

obtained and generated that are part of procedure E/12527/2021" was also

erroneous, there being no other procedure or documents of which Bankinter has

proof (otherwise, the Agency is requested to provide Bankinter with this

"it will be remedied

information together with the complete administrative file); and

formally said error, so that said Agreement is rectified in the file".

On 02/07/2022, the defendant was notified of the Commencement Agreement

Sanctioning Procedure, appearing in the header of the same the reference to the

File No.: EXP202104875, that is, the same one that appears in the Proposal that is

issues and numbering produced by the internal system.

Subsequently, the defendant has requested a copy of the file and will have been able to

verify that the documents that make up the administrative file are

correspond to those provided by the claimant, those generated by the AEPD and the

provided by the claimant.

Likewise, on 03/29/2022 the opening of the test period was notified and the

Contrary to the previous letter, there is a reference to the disciplinary procedure

File No. PS/00634/2021 and in the second point of the AGREEMENT, it is indicated

requirement that the defendant himself indicated in his allegations to the initiation agreement; in

regarding the reference to the aforementioned numbers both of the disciplinary procedure

and the file are figures provided by the internal application system and that nothing

have to do with different files (thus the number of disciplinary procedure

is a code number provided by the system in relation to the file

procedural) but that have nothing to do with files or documents other than

those that the defendant has in his possession and that are part of the file

administrative, so there is no other procedure or other documentation of

which Bankinter is not aware of.

In short, the unique file number that appears on the settlement agreement

home includes all the internal numbers that identify the procedures carried out with



above, which all refer to the same claim; what he could

check upon receipt of the copy of the entire file

2. As we pointed out in the previous foundation, article 5, Principles

regarding treatment, establishes in its letter f) the following:

“The personal data will be:

(…)

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

personal data, including protection against unauthorized or unlawful processing and

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

appropriate technical or organizational ("integrity and confidentiality")

(…)”

What the GDPR comes to point out is that the technical and organizational measures

adopted must be aimed at preventing unauthorized access or use of said

data and the equipment used in the treatment.

In this same sense, Recital 39 states that "... All

reasonable measures to ensure that the data is rectified or deleted

personal information that is inaccurate. Personal data must be processed in a way that

ensure adequate security and confidentiality of personal data,

including to prevent unauthorized access or use of such data and equipment

used in treatment.

This principle is reinforced in recital 49 of the GDPR, stating that the

processing of personal data will be carried out..."to the extent strictly necessary

and provided to ensure the security of the network and information, that is, the

capacity of a network or an information system to resist, at a certain level

of trust, to accidental events or illegal or malicious actions

that compromise the availability, authenticity, integrity and confidentiality of the

personal data stored or transmitted (…).”

The documentation in the file offers clear indications that the

claimed, violated article 5 of the GDPR, duty of confidentiality, by enabling the

visualization in your monthly bank statement, not only the movements of your

account, but also those relating to a third person.

As it appears in the proven facts, a copy of the extract is provided

comprehensive monthly corresponding to June 2021 in which the movements of

the account of which the claimant is the holder, as well as the movements related to

a second account owned by a third person.

The duty of confidentiality, previously the duty of secrecy, must

understood that its purpose is to prevent leaks of data not

consented by the holders of the same.

The duty of confidentiality is an obligation that is incumbent not only on the

responsible and in charge of the treatment but to anyone who intervenes in any

treatment phase and complementary to the duty of professional secrecy.



The defendant himself in his brief of 04/07/2022 has stated that "In

Actually, the situation was caused by an error when managing the change of

ownership of the Other Account (as the Claimant himself stated in the Brief).

Access to the Other's information had not been completely withdrawn.

Account (of which he had been co-owner) at the time of the change of ownership of the

itself, to the extent that the information that

appeared in the Claimant's "monthly statement" document, to exclude that

regarding the Other Account" and, furthermore, that "when he received the Transfers of

Complaint and Information Request, Bankinter was able to understand exactly what

happened, undoing the previous misunderstanding and adopted measures to solve the

incidence" (underlining corresponds to the AEPD).

Therefore, it is considered that the defendant is responsible for the infringement of the

article 5.1.f) of the RGPD, infringement typified in its article 83.5.a) of the aforementioned

regulation.

IV.

Article 83.5 a) of the GDPR, considers that the infringement of "the principles

principles for treatment, including the conditions for consent under

of articles 5, 6, 7 and 9" is punishable, in accordance with section 5 of the

mentioned article 83 of the aforementioned GDPR, "with administrative fines of €20,000,000

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

maximum of the overall annual total turnover of the previous financial year,

opting for the one with the highest amount".

The LOPDGDD in its article 72 indicates: "Infractions considered very serious:

1. Based on what is established in article 83.5 of the Regulation (EU)

2016/679 are considered very serious and the infractions that

suppose a substantial violation of the articles mentioned in that and, in

particular, the following:

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

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

(…)"

Secondly, article 32 of the GDPR "Security of treatment",

V

states that:

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

nature, scope, context and purposes of processing, as well as risks of

variable probability and severity for the rights and freedoms of individuals

physical, the person in charge and the person in charge of the treatment will apply technical and

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

which may include, among others:

a) the pseudonymization and encryption of personal data;



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

permanent resilience of treatment systems and services;

c) the ability to restore availability and access to data

quickly in the event of a physical or technical incident;

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

technical and organizational measures to guarantee the safety of the

treatment.

2. When evaluating the adequacy of the level of security, particular attention should be paid to

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

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

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

unauthorized access to such data.

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

certification mechanism approved under article 42 may serve as an element

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

present article.

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

ensure that any person acting under the authority of the controller or the

manager and has access to personal data can only process such 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".

SAW

The violation of article 32 of the GDPR is typified in article

83.4.a) of the aforementioned GDPR in the following terms:

"4. Violations of the following provisions will be penalized, according to

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

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

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

the highest amount:

a) the obligations of the person in charge and the person in charge according to articles 8,

11, 25 to 39, 42 and 43.

(…)”

For its part, the LOPDGDD in its article 73, for prescription purposes, qualifies

of "Infringements considered serious":

Based on what is established in article 83.4 of Regulation (EU) 2016/679

“

are considered serious and will prescribe after two years the infractions that suppose a

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

following:

(…)

g) The breach, as a consequence of the lack of due diligence,

of the technical and organizational measures that have been implemented in accordance with



to what is required by article 32.1 of Regulation (EU) 2016/679”.

(…)”

The facts disclosed in this claim materialize

also in the breach of technical and organizational measures, violating the

data confidentiality.

1. The GDPR defines personal data breaches 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.”

VII

The documentation provided to the file shows that the defendant has

violated article 32 of the GDPR, when a security incident occurred by allowing

access to the claimant to the personal data of a third party, when viewing in their area

personnel from the entity's website the movements of another person's account.

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

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

object of treatment, but it establishes that the person in charge and the person in charge of the

treatment will apply technical and organizational measures that are appropriate to the risk

that entails the treatment, taking into account the state of the art, the costs of

application, 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 risk detected, noting that the determination of the measures

technical and organizational procedures must be carried out taking into account: pseudonymization and

encryption, the ability to ensure confidentiality, integrity, availability and

resiliency, the ability to restore availability and access to data after a

incident, verification process (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

this Regulation, the controller or processor must assess the risks

inherent to the treatment and apply measures to mitigate them, such as encryption. Are

measures must ensure an adequate level of security, including the

confidentiality, taking into account the state of the art and the cost of its application

regarding the risks and nature of the personal data to be

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



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

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

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

authorized to said data, susceptible in particular to cause damages

physical, material or immaterial.

2. In the present case, the defendant has alleged that he has granted a special

relevance to the protection of the confidentiality of the information under its control, for

which has developed codes, policies and procedures aimed at guaranteeing the

protection of said information, listing below a series of measures

implanted, surprising him that the AEPD accused him of a violation of art. 32 GDPR.

However, such a statement cannot be accepted; it seems obvious that said

incident has occurred, that is, the technical and organizational measures implemented
failed due to a security incident when allowing the visualization by the
claimant of the movements of the account of a third party in his personal area of the
website of the entity, violating the principle of confidentiality.

In accordance with the proven facts and the documentation contained in the
file, the claimant addressed the defendant by sending him an e-mail on 07/16/2021,
stating that "Yesterday ... I accessed my personal account on the website of
Bankinter in order to consult a payment made last month. Was
reviewing the movements of my account when, what is my surprise to discover that
The movements of another account of which I am not the owner also appear. that other
According to the figure, the account corresponds to a "current or pension account...
I sense that the person who owns that gold pension account is the person with whom
share the ownership of a payroll account where we deposited our
corresponding payroll (my ex-partner). A possible explanation of these facts, the
more predictable, is that during the steps taken at the time by the office of
Bankinter so that we could put an end to joint ownership of the payroll account and pass
to each have their own payroll account, there was some oversight on the part of the
bank office...

In accordance with the foregoing, I request that you proceed to the immediate correction of
this situation".

Six days later, on 07/22/2021, the defendant responded by stating:

"We proceeded to carry out the appropriate steps based on the situation raised"

Well, despite the fact that the situation raised by the claimant was
crystal clear did not receive any response, stating that "The situation that
I exposed it to the bank, it continues the same without being corrected".

Response that does not differ much from that carried out on 08/19/2021 by the

claimed to the claimant "In relation to the situation raised by you, I

We inform you that we have forwarded your comments to those responsible

of their accounts to deal with this matter", and which was provided on 12/27/2021

In response to the information request from the AEPD to which we referred in the

point 1 of FD III.

Therefore, the defendant cannot rely on the fact that it was not until he received

the Complaint Transfers and Request for Information when you could understand



exactly what happened, adopting measures to solve the incident because the

The claimant in his claim document and in the extracts provided made it clear:

identified the type of account: "That other account, as shown, corresponds to a

account "current gold pension..." and to the owner of the same "I sense that the person who owns

of that gold pension account is the person with whom to share the ownership of a

payroll account where we entered our corresponding payroll (my

ex partner)..,".

The Supreme Court in a judgment of 02/15/2022 states that: "The obligation to

adopt the necessary measures to guarantee the security of personal data

cannot be considered an obligation of result, which implies that produced a

leaking of personal data to a third party there is responsibility regardless

of the measures adopted and the activity carried out by the person responsible for the file

or the treatment.

In the obligations of result there is a commitment consisting of the

fulfillment of a certain objective, ensuring the achievement or proposed result,
In this case, guarantee the security of personal data and the absence of
security leaks or breaches.
In obligations of means, the commitment acquired is to adopt
technical and organizational means, as well as deploy diligent activity in its
implantation and use that tends to achieve the expected result with
that can reasonably be classified as suitable and sufficient for its achievement,
for this reason they are called obligations "of diligence" or "of behavior".
The difference lies in the responsibility in both cases, because while
that the obligation of result responds to a harmful result due to the failure of the
security system, whatever its cause and the diligence used. In the
obligation of means is enough to establish technically appropriate measures and
implement and use them with reasonable care.
In the latter, the sufficiency of the security measures that the
responsible has to establish has to be related to the state of technology
at all times and the level of protection required in relation to the data
treated, but a result is not guaranteed."
The Court confirms that the design of the technical means is not sufficient
and organizational requirements, since it is also necessary to correctly
implementation and proper use.
Therefore, the responsibility of the defendant is determined by the incident
of security revealed by the claimant, since he is responsible for taking
decisions aimed at effectively implementing the technical and
appropriate organizational measures to guarantee a level of security appropriate to the risk
to ensure the confidentiality of the data, restoring its availability and preventing
access to them in the event of a physical or technical incident. However, from the

documentation provided shows that the entity has not only breached this

obligation, but also the adoption of measures in this regard is unknown, despite

of having given transfer of the claim presented.

Pursuant to the foregoing, it is estimated that the defendant would be

allegedly responsible for the infringement of the GDPR: the violation of article 32,

offense typified in article 83.4.a).



The defendant alleges the existence of a medial contest of infractions for

concur the assumption referred to in art. 29.5 of Law 40/2015, of October 1,

Therefore, the imposition of only one of the two sanctions would proceed, specifically, the

regarding the violation of article 5.1.f) of the GDPR.

VIII

The art. 29.5 of Law 40/2015, of October 1, on the Legal Regime of the Sector

"When the commission of an offense derives

Public, establishes that:

necessarily the commission of another or others, only the sanction must be imposed

corresponding to the most serious offense committed".

However, such argumentation cannot be accepted; the specific standard in

data protection, that is, the GDPR, establishes in its article 83.3 that:

"3. If a person in charge or a person in charge of the treatment fails to comply

intentionally or negligently, for the same treatment operations or operations

related parties, various provisions of this Regulation, the total amount of the

administrative fine shall not exceed the amount provided for the most serious offences.

serious.

We already pointed out in FD IV that the processing of personal data

violating the principles and guarantees established in article 5 of the GDPR,

considered as a very serious infraction, so the only limit would be established by

the amount indicated in article 83.5 of the GDPR "€20,000,000 maximum 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 one with the highest value".

In order to establish the administrative fine that should be imposed, the

observe the provisions contained in articles 83.1 and 83.2 of the GDPR, which

point out:

IX

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

administrative proceedings under this article for violations of this

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

effective, proportionate and dissuasive.

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

of each individual case, as an addition to or substitute for the measures contemplated

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

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

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

nature, scope or purpose of the processing operation in question

as well as the number of stakeholders affected and the level of damage and

damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor

to alleviate the damages and losses suffered by the interested parties;



d) the degree of responsibility of the controller or the person in charge of the

processing, taking into account the technical or organizational measures that have

applied under articles 25 and 32;

e) any previous infringement committed by the person in charge or in charge of the

treatment;

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

remedy the breach and mitigate the potential adverse effects of the breach;

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

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

particularly if the person in charge or the person in charge notified the infringement and, in such a case,

what extent;

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

previously ordered against the person in charge or in charge in question

in relation to the same matter, compliance with said measures;

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

of certification approved in accordance with article 42, and

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

case, such as the financial benefits obtained or the losses avoided, direct

or indirectly, through the infringement.

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

Article 76, "Sanctions and corrective measures", establishes that:

"2. In accordance with the provisions of article 83.2.k) of the Regulation (EU)

2016/679 may also be taken into account:

a) The continuing nature of the offence.

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

of personal data.

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

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

commission of the offence.

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

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

f) The affectation of the rights of minors.

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

data.

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

voluntary, alternative conflict resolution mechanisms, in those

cases in which there are controversies between those and any

interested."

- In accordance with the transcribed precepts, and without prejudice to what results from

the instruction of the procedure, in order to set the amount of the fine to

impose in the present case for the infringement typified in article 83.5.a) and article

5.1.f) of the GDPR for which the defendant is held responsible, in an initial assessment,

consider the following factors concurrent:

They are aggravating circumstances:

- The nature, seriousness and duration of the infringement: the facts considered

proven seriously affect a basic principle in the treatment of data of



personal nature, such as confidentiality and integrity, and whose reproach is

more seriousness revealing the data of the account of a third party, type data

economic; damages caused as a result of interference in the

privacy sphere of the claimant, since we must not forget that we are

in the event of the infringement of a fundamental right to the protection of personal data and

that the claimant has been forced to file a claim with the AGPD before the

inaction of the defendant.

- The activity of the allegedly infringing entity is linked to the

data processing of both clients and third parties. In the activity of the entity

claimed, the processing of personal data is essential, therefore,

given the volume of business of the same the importance of the conduct object of the

This claim is undeniable (article 76.2.b) of the LOPDGDD in relation to the

article 83.2.k).

- Although it cannot be argued that the defendant acted

intentionally, there is no doubt that there is a serious lack of diligence in

his performance. Connected with the degree of diligence that the data controller

is obliged to deploy in compliance with the obligations imposed by the

data protection regulations, the SAN of 10/17/2007 can be cited. although it was

issued before the entry into force of the GDPR, its pronouncement is perfectly

extrapolated to the assumption that we analyse. The ruling, after alluding to the fact that the

entities in which the development of their activity entails a continuous treatment of

data of clients and third parties must observe an adequate level of diligence,

specified that "(...) 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. And in assessing the degree of diligence must

especially the professionalism or not of the subject should be considered, and there is no doubt that,

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

copious handling of personal data must insist on rigor and

exquisite care to comply with the legal provisions in this regard" (article 83.2,

b) of the GDPR).

- The volume of business of the defendant is one of the entities

leading financial institutions in the Spanish market, by business purpose (article

83.2, k) of the GDPR).

Extenuating circumstances are considered:

- Only one person has been affected by the infringing conduct.

In accordance with the above factors, it is deemed appropriate to impose on the defendant

for violation of article 5.1.f) of the GDPR, a penalty of 60,000 euros.

- In accordance with the precepts transcribed, for the purpose of setting the amount of the

sanction of a fine to be imposed in the present case for the offense typified in the



Article 83.4.a) and Article 32.1 of the GDPR for which the defendant is held responsible, in

In an initial assessment, the following factors are considered concurrent:

They are aggravating circumstances:

- The nature, seriousness and duration of the infringement: the facts considered
proven affect a basic issue in data protection such as the
security of the same, allowing the access of the claimant to the data of a
third, his ex-partner, as a consequence of the security incident and his absence from
response, initially, to the claim filed by the claimant, which
motivated him to contact the AEPD (article 83.2, a) of the GDPR).

- The activity of the allegedly infringing entity is linked to the
data processing of both clients and third parties. In the activity of the entity
claimed, the processing of personal data is essential, therefore,
given the volume of business of the same the importance of the conduct object of the
This claim is undeniable (article 76.2.b) of the LOPDGDD in relation to the
article 83.2.k).

- Although it cannot be argued that the defendant acted
intentionally, there is no doubt that there is a serious lack of diligence in
his performance. Connected with the degree of diligence that the data controller
is obliged to deploy in compliance with the obligations imposed by the
data protection regulations, the SAN of 10/17/2007 can be cited. although it was
issued before the entry into force of the GDPR, its pronouncement is perfectly
extrapolated to the assumption that we analyse. The ruling, after alluding to the fact that the
entities in which the development of their activity entails a continuous treatment of
data of clients and third parties must observe an adequate level of diligence,
specified that "(...) 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. And in assessing the degree of diligence must
especially the professionalism or not of the subject should be considered, and there is no doubt that,

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

copious handling of personal data must insist on rigor and

exquisite care to comply with the legal provisions in this regard" (article 83.2,

b) of the GDPR).

- The volume of business of the defendant is one of the entities

leading financial institutions in the Spanish market, by business purpose (article

83.2, k) of the GDPR).

Extenuating circumstances are considered:

- Only one person has been affected by the infringing conduct.



In accordance with the above factors, it is deemed appropriate to impose on the defendant

for violation of article 32.1 of the GDPR a penalty of 40,000 euros.

In view of the foregoing, the following is issued

PROPOSED RESOLUTION

FIRST. That by the Director of the Spanish Data Protection Agency

penalize BANKINTER, S.A., with NIF A28157360, for a violation of article

5.1.f) of the GDPR, typified in article 83.5, a) of the GDPR, with a fine of €60,000

(sixty thousand euros).

SECOND. That by the Director of the Spanish Data Protection Agency

penalize BANKINTER, S.A., with NIF A28157360, for a violation of article

32.1 of the GDPR, typified in article 83.4, a) of the GDPR, with a fine of €40,000

(forty 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 total sanction would be established at €80,000 (eighty thousand euros) and its payment will imply the termination of the procedure. The effectiveness of this reduction will be conditioned to the withdrawal or resignation of any action or appeal via administrative 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 depositing it in the restricted account no. ES00 0000 0000 0000 0000 0000 open in the name of the Spanish Data Protection Agency in the entity 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, reduction of the amount of the sanction. You must also send the Proof of admission to the Sub-Directorate General of Inspection to proceed to close The file.

In accordance with the provisions of article 76.4 of the LOPDGDD and given that the amount of the sanction imposed is greater than one million euros, it will be subject to publication in the Official State Gazette of the information that identifies the offender, the infraction committed and the amount of the sanction.

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.

R.R.R.

EXHIBIT

File index EXP202104875

10/08/2021 A.A.A.

10/11/2021 A.A.A.

11/24/2021 Transfer of claim to BANKINTER, S.A.

11/25/2021 Transfer of claim 2 to BANKINTER, S.A.

12/27/2021 Allegations by BANKINTER, S.A.

12/29/2021 Admission for processing to A.A.A.

02/02/2022 Opening of BANKINTER, S.A.

02/07/2022 Information. Claimant to A.A.A.

02/09/2022 Term extension request from BANKINTER S.A

02/09/2022 Request for term extension from BANKINTER.S. TO

02/11/2022 Amp. Term to BANKINTER, S.A.

02/14/2022 Request for a copy of the BANKINTER.S file. TO

02/14/2022 Transfer to BANKINTER, S.A.

02/25/2022 Allegations of BANKINTER.S. TO

03/29/2022 Test period notification

>>

SECOND: On September 22, 2022, the claimed party has proceeded to the

payment of the penalty in the amount of 80,000 euros using 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

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

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 EXP202104875, 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

968-230822

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es