 File No.: EXP202202178

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 March 15, 2023, the Director of the Spanish Agency for

Data Protection agreed to initiate sanction proceedings against BANKINTER

CONSUMER FINANCE E.F.C., S.A. (hereinafter, the claimed party), through the

Agreement transcribed:

<<

File No.: EXP202202178

AGREEMENT TO START THE SANCTION PROCEDURE

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

based on the following

FACTS

FIRST: D.A.A.A. (hereinafter, the claiming party) on December 31,

2021 filed a claim with the Spanish Data Protection Agency. The

claim is directed, initially, against LINEA ASEGURADORA and against

BANKINTER S.A. The reasons on which the claim is based are the following:

The claimant states that, a year and a half ago, he contracted the Línea

Directa Bankintercard linked to your bank account, proceeding to its activation and

stating, as associated address, that of his habitual residence in Madrid.

On November 4 and 5, 2021, the claimant verifies that, through

said card, several cash withdrawals had been made through an ATM located

in the town of Vigo, as well as various payments.

After what happened, he contacted the claimed entity and it informed him that they had

issued a duplicate of the claimant's card and that they had sent it to

his supposed address (in Vigo).

He states that he has complained several times about what happened; since, it has been issued

a duplicate of the card you own, without your consent, in addition to sending it

to an address other than his own, but he has not received a response in this regard.

Along with the claim, the following is provided:

Card photography.

-

- Screenshot of the activation of the card (in which it appears as address

associated: ***ADDRESS.1).

- Screenshot of the fraudulent operations carried out.

- Screenshot of the App, user area, (in which an address appears

associated with the different card, now showing an address in Vigo:

***ADDRESS.2).

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

hereafter LOPDGDD), said claim was forwarded to BANKINTER S.A., for

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

actions carried out to adapt to the requirements established in the regulations of

Data Protection.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of October 1, of the Common Administrative Procedure of the Administrations Public (hereinafter, LPACAP), was notified on February 21, 2022, as It appears in the certification that is in the file.

On March 14, 2022, this Agency received a written response indicating that "…after analyzing the information provided by the Complainant, we have verified that Bankinter has no contractual relationship with Mr. A.A.A.. From In fact, as we will prove below, Bankinter S.A does not market the type of credit cards referenced in your claim. Of the investigations carried out we have verified that said card is marketed by our consumer subsidiary Bankinter Consumer Finance E.F.C, S.A. As we have just explained, it has been proven that between the There is no contractual relationship between the claimant and Bankinter, since the card that is the object of controversy has been issued by Bankinter Consumer Finance, E.F.C., S.A. By Therefore, Bankinter cannot make any decision on the purpose of this claim, since it does not hold the status of data controller and has not intervened in the process of issuing the card contracted by the Claimant, nor has information in this regard on the process of issuing a duplicate."

THIRD: 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 LINEA DIRECTA ASEGURADORA CIA DE SEGUROS Y REASEGUROS SA to proceed with its analysis and inform this Agency within a month of the actions carried out carried out to adapt to the requirements established in the data protection regulations.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of

October 1, of the Common Administrative Procedure of the Administrations

Public (hereinafter, LPACAP), was notified on February 21, 2022, as

It appears in the certification that is in the file.

On March 17, 2022, this Agency received a written response

indicating that "…That the claim is not related to this entity, since

The issuance of credit cards is an activity reserved for certain merchants,

payment service providers, and LÍNEA DIRECTA ASEGURADORA S.A. it's not

a credit institution or a payment service provider, but rather an entity

insurance carrier.

- That the issuer of the card is BANKINTER CONSUMER FINANCE E.F.C., S.A.

- That the card includes the LÍNEA DIRECTA brand as mere sponsorship…"

FOURTH: On March 31, 2022, in accordance with article 65 of the

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

directed against BANKINTER CONSUMER FINANCE E.F.C., S.A., (hereinafter,

BANKINTER CF).

FIFTH: The General Sub-directorate of Data Inspection proceeded to carry out

preliminary investigation 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:

RESULT OF INVESTIGATION ACTIONS

On June 8, 2022, additional information is requested from the complaining party,

both to the natural person and to the person who submitted the claim on their behalf,

to provide evidence of the communications you have maintained with the

claimed part and that have not been answered.

The postal notification to the natural person is collected on June 15, 2022,

while the notification to the person who filed the claim is accepted with

dated June 9, 2022.

Although, no reply has been received.

Using the bank account number provided by the claimant, the

at https://www.iban.es the name of the bank through its bank entity code and

it is found that the entity is BANKIA, S.A., now integrated into CAIXABANK, S.A.

Asked about the ownership of the bank account, as well as about the relationship with

BANKINTER CF, dated June 23, 2022, CAIXABANK, S.A sends this

Agency the following information and statements:

- That the account number referred to by the claimant is the new numbering in

CAIXABANK, S.A. from an account that initially belonged to BANKIA, S.A. The

ownership of the account corresponds to the claimant.

- That CAIXABANK, S.A. does not maintain a relationship with BANKINTER CF for the issuance

Of cards.

- That there is no relationship between CAIXABANK, S.A. and BANKINTER CF for the

granting and activation of cards and therefore no protocol has been developed

some.

Once a first request for information has been made to BANKINTER CF, the latter sends, with

dated June 22, 2022 (entry registration number in the AEPD

REGAGE22e00025885620), a statement of allegations that includes:

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

4/17

- Confirmation that the ownership of the bank card object of the claim

belongs to the claimant.

- The extract dated November 2021 of the card indicated by the claimant,

where the veracity of the facts claimed is confirmed: two withdrawals of

cash through an ATM in Vigo and two payments in that town.

-

The claimed party acknowledges that there has been identity theft: “[…]

This action, due to the client's claim, was considered carried out due to an alleged

supplanter”.

- BANKINTER CF indicates that it has "a customer identification system

for your connection to the telephone service, based on the ID number plus a

4-digit Personal Access Code (CAP), known only to the customer. In it

In the event that the client does not remember this code, questions are asked

security (date of birth, full address, telephone number and bank

where the card is domiciled) and a new CAP is assigned.”

- BANKINTER CF details the card application procedure online:

First of all, the client must enter their Client Area on the web

www.bankinterconsumerfinance.com. To access your Customer Area you must

Identify yourself in advance by entering your username and password.

Once you have accessed the Customer Area, you must select the option

“Block card” in the available operating menu.

Once the reason is indicated, you are presented with the action confirmation screen

that you have applied for, indicating that a new card will be issued. In this

screen, you must enter the 6-digit OTP that has been sent to the mobile phone

the client's.

On July 18, 2022 (entry registration number in the AEPD

REGAGE22e00030983051), the claimed party sends this Agency a letter of

response to the second information requirement that includes:

-

-

"Customer Identification Procedure Manual in customer service

telephone service”, which regulates telephone action for the identification and modification of

of the personal data of its clients through telephone channels and that includes the

arguments and instructions provided to telephone operators who

manage these processes.

Information about the postal delivery of payment cards. refer part

claimed that uses a standard or ordinary modality for sending the

cards, no certificate. In order for a customer to use the card, it is

It is necessary to activate it previously and there are two methods to do this:

o Web channel, in which the client must enter their username and password in

the customer area and then enter the signature OTP of the

operation, sent by SMS to the associated telephone number.

o Telephone channel, after being identified as explained above.

- Copies of the recordings of the telephone calls made.

-

The claimed party states that no notice was sent by SMS to the number

number Tfno_inicial or through another channel informing of the change of telephone number and incident

in which "customers can consult at any time what are the data

of contact that they have informed in their "Customer Area"".

On November 10, 2022 (entry registration number in the AEPD

REGAGE22e00051124905), the claimed party sends this Agency a response

to the third information requirement with the following information and statements:

-

The Entity does not allow the change of passwords to access the web application

through telephone channels.

- The change of passwords to access the web application can only be

carried out through the web environment itself, in accordance with the procedure

described in the "User Generation and Reactivation Procedure Manual

on Web/App”

-

Information on the claimant's password change requests for the

web access that have been received from January 1, 2020 to the present,

along with the evidence associated with said requests and the details of the

information collected to prove the identity of the claimant.

On October 3, 2022, additional information is requested from the complaining party,

both to the natural person and to the person who submitted the claim on their behalf,

to provide information on whether a complaint has been filed with the police

denunciation of this identity theft that is being claimed and indications

about a possible loss of your personal data.

The postal notification to the natural person is collected on October 11, 2022,

while the notification to the person who filed the claim is accepted with

date October 4, 2022.

Although, no reply has been received.

CHRONOLOGICAL DESCRIPTION OF THE EVENTS

1. On February 6, 2018, at the client's request, the issuance of

the card numbered ***NUMBER.1, which is the card that is the object of the claim,

which is activated on the client website on February 7, 2018, prior

correct introduction of the connection username and password and the OTP signature of

the operation, sent to the telephone number Tfno_inicial.

The claimed party facilitates the screenshot of the logs of this operation, in

which shows the verification of the OTP signature of the operation, sent to the

active telephone number of the claimant, Tfno_inicial.

1. On October 26, 2021 at 5:25 p.m., by telephone call to the

customer service and after identification, the telephone number is added

Tfno_supl_1 as the new contact telephone number for the operator that

answered the call, with user number SO17186. Telephone Modification.

The claimed party provides as evidence the copy of the recording of the

phone call, which will be analyzed later in this report.

2. Regarding address changes, dated October 26, 2021 at

23:05h is added as postal address: ***ADDRESS.2. Said modification is

made through the customer website, after correctly entering the username and password

of connection and of the OTP of signature of the operation, sent for this purpose to the number of

phone number_suppl_1. Postal Address Modification.

The claimed party facilitates the data modification procedure through the

customer website, as well as the screenshot of the logs of this operation, in

which shows the correct authentication of the user (prior introduction of the

username and password) and verification of the OTP signature of the operation,

sent to the claimant's active telephone number (in this case, the

telephone number of the alleged impersonator Tfno_supl_1). It also provides capture

screen of the shipment and delivery logs of the signature OTP to the telephone number

Phone_supp_1.

3. On October 27, 2021 at 09:11 a.m., by phone call to the

customer service and after identification, the deletion of the

numbers ***PHONE.1 and Phone_initial; remaining as the only number of

contact the Tfno_supl_1. Said deletion is executed by the operator who attended

the call, with user number AAXXXXX. Telephone Modification.

The requested party delivers as evidence the copy of the recording of the call

telephone.

4. On October 27, 2021 at 09:37 a.m., on the client website (loss of the

card), the card (…) is automatically issued as a replacement for the previous one.

ISSUANCE OF THE CARD.

The claimed party facilitates the screenshot of the logs of this operation, in

which shows the verification of the OTP signature of the operation, sent to the

claimant's active phone number (in this case, the phone number of the claimant)

presumed impersonator Tfno_supl_1). It also provides screenshot of

the sending and delivery logs of the signature OTP to the telephone number Tfno_supl_1.

5. On October 27, 2021 at 12:43 p.m., a request for

modification of the user's keys, which is executed by means of the correct

introduction of the OTP code sent by SMS to the telephone number Tfno_supl_1.

The claimed party provides evidence of this operation: fingerprint, OTP shipment

and traces.

6. This card issued on October 27, 2021 is activated by the customer website

dated November 3, 2021, after correct user input and

connection password and the OTP for signing the operation, sent to the phone

Tfno_supl_1, and is the one with which the operations of days 4 and 5 of

November 2021. Activation of the card.

The claimed party facilitates the screenshot of the logs of this operation, in

which shows the verification of the OTP signature of the operation, sent to the

claimant's active phone number (in this case, the phone number of the claimant)

presumed impersonator Tfno_supl_1). It also provides screenshot of

the sending and delivery logs of the signature OTP to the telephone number Tfno_supl_1.

7. On November 3, 2021, on the customer website, the password is changed

access to the web application on three occasions (4:25 p.m., 5:30 p.m. and 5:50 p.m.) through

of the correct introduction of the three OTP keys –one for each request for

modification – which are sent by SMS to the telephone number Tfno_supl_1.

Change of password.

The claimed party provides evidence of these operations: fingerprint, shipping

OTP and traces.

8. On November 5, 2021, by telephone call to the services of

customer service, and after identification, it is re-established as unique

contact phone number the initial_phone. This change is executed by the

operator who answered the call, with user number BBXXXXX. Modification

Telephone by the claimant.

9. On this same date, November 5, 2021, the password change is requested

on the client website three times, two successful and one unsuccessful:

At 3:48 p.m., using the OTP key entered correctly and sent by SMS to

telephone number Tfno_supl_1, the access password is modified. Change of

password.

At 4:16 p.m., through the OTP entered correctly and sent by SMS to

phone number Phone_initial, the access password is modified again.

Change of password by the claimant.

Subsequently, at 4:29 p.m., a new password change is requested, but

this was not carried out since the OTP key sent to the telephone number

phone_initial was not entered. Password change attempt.

The claimed party provides evidence of these operations: fingerprint, shipping

OTP and traces.

10. With dates November 8 and 22, 2021, February 22, 2022 and March 23,

2022, on the customer website, the password to access the web application is changed to

11:21 a.m., 2:20 p.m., 3:17 p.m. and 9:58 a.m. respectively, through the correct

introduction of OTP keys sent by SMS to the phone number

phone_initial. Change of password by the claimant.

The claimed party provides evidence of these operations: fingerprint, shipping

OTP and traces.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

11. On April 11, 2022 at 6:25 p.m., it is sent to the telephone number

Phone_initial an OTP key to change the access password, which is not

introduced. Password change attempt.

By phone call to customer service, and after the

identification, the telephone is replaced by Tfno_supl_2. Said change is

executed by the operator who answered the call, with user number

CCXXXXX. Telephone Modification.

Finally, at 18:43 a new OTP key is sent to the phone number

Tfno_supl_2, which is entered correctly and, therefore, the last one is materialized

change of password. Change of password.

The claimed party provides evidence of currency exchange operations

password: fingerprint, OTP sending and traces; and the screenshot of the data

of the claimant modified on that date, as well as the copy of the recording of the

phone call.

12. Between April 12 and 20, 2022, three cards are automatically issued as

replacement of the previous ones due to loss of the card, blocked on the website of

customers. These cards have not been activated.

13. On May 3, 2022, the following is added as a postal address: ***ADDRESS.3.

Said modification is made through the client's website, after correct introduction

the connection username and password and the OTP for signing the operation,

sent for this purpose to the telephone number Tfno_supl_2. Address Modification

Postcard.

The claimed party provides as evidence the screenshot of the logs of

this operation, in which the correct authentication of the user is appreciated (prior

entering the username and password) and checking the OTP signature of the

operation, sent to the claimant's active telephone number (in this case, the

telephone number of the alleged impersonator Tfno_supl_2). It also provides

screenshot of the shipping and delivery logs of the signing OTP to the number of

phone phone_suppl_2.

14. On that same date, May 3, 2022, they are automatically issued again

two cards to replace the previous ones due to loss of the card,

blocked on the client website. These cards have not been activated.

15. On May 6, 2022, after knowing the impersonation of the client, it becomes

to restore as contact telephone number the Initial_Telephone. Modification of

Phone.

The claimed party facilitates the screenshot of the claimant's data

modified on that date.

16. Finally, on May 9, 2022, after learning of the impersonation of the

client, it is reset as unique client address ***ADDRESS.1.

Postal Address Modification.

17. Subsequently, the product is cancelled.

EVIDENCES

In the chronological description of the events, the operations have been presented

carried out on the claimant's data together with the evidence provided by the

party claimed for each of the operations.

In the recording of the call made on October 26, where the

Tfno_supl_1 as the new contact telephone number, the user's identification

It is done by the correct answer to the following security questions:

- ID

- Full name

- Birthdate

- Full address, including zip code

- Mobile phone

- Bank through which the receipts are passed. Bank responds.

In the recording, a new CAP number is generated: XXXX and the number of

mobile phone to operate with it in the future. The number is also removed from the profile

associated landline number.

The alleged impersonator has prior knowledge of all the data of the claimant.

In the recording of the call made on October 27, where the deletion is requested

of the numbers ***TELEPHONE.1 and Phone_initial and Phone_supl_1 remains as unique

contact number, user identification is made by presenting

of the CAP number generated the day before.

In the recording of the call made on April 11, where Tfno_supl_2 is added,

the identification of the user is done by presenting the same number

CAP generated by the alleged impersonator in October 2021.

The voices on all three recordings seem to belong to the same person, so

it follows that there were again impersonation attempts in May 2022.

Regarding the evidence collected in relation to the identification of the claimant

when you made the password change requests, the complained party indicates that

No user authentication "log" is kept prior to the change of the

access passwords, since they were modified through the procedure

key reset procedure mentioned above.

SECURITY MEASURES IMPLEMENTED AT THE TIME OF THE

FACTS:

- To access the telephone service and modify the telephone number

associated mobile phone, the presumed impersonator had to know either the CAP or the

following personal data of the claimant:

• Full name

• D.N.I. or residence card

• Birthdate

• Full address

• Landline and/or mobile phone

It is considered weak security. If one layer of security fails, the second layer of

security should be at least as secure as the first. The CAP is a number of

4 digits, that is, there are 10,000 possibilities.

As of May 2022 it is no longer possible to change the telephone number of the

customers through the telephone channel.

- To access the private Web space or the BANKINTER CF App, the alleged

impersonator had to know the username and password. If you didn't have the password, you could

generate a new one knowing D.N.I./N.I.F. and date of birth and entering the

OTP sent to the associated mobile phone (two-step authentication).

The strength of this security measure lies in the second step of the

authentication (sending the OTP to the reported mobile phone), but the presumed

impersonator had previously modified that phone number.

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

breached obligation

Article 58 of the GDPR, Powers, states:

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

indicated below:

(…)

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

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

particular;(…)".

Article 6, Legality of the treatment, of the GDPR in its section 1, establishes that:

"1. Processing will only be lawful if at least one of the following is fulfilled

conditions:

a) the interested party gave his consent for the processing of his personal data

for one or more specific purposes;

b) the treatment is necessary for the execution of a contract in which the interested party

is part of or for the application at the request of the latter of pre-contractual measures;

c) the processing is necessary for compliance with a legal obligation applicable to the

responsible for the treatment;

d) the processing is necessary to protect vital interests of the data subject or of another

Physical person;

e) the treatment is necessary for the fulfillment of a mission carried out in the interest

public or in the exercise of public powers conferred on the data controller;

f) the treatment is necessary for the satisfaction of legitimate interests pursued

by the person in charge of the treatment or by a third party, provided that on said

interests do not outweigh the interests or fundamental rights and freedoms of the

interested party that require the protection of personal data, in particular when the

interested is a child.

The provisions of letter f) of the first paragraph shall not apply to the treatment

carried out by public authorities in the exercise of their functions".

On the other hand, article 4 of the GDPR, Definitions, in its sections 1, 2 and 11, indicates

that:

"1) «personal data»: any information about an identified natural person or

identifiable ("the data subject"); An identifiable natural person shall be considered any person

whose identity can be determined, directly or indirectly, in particular by means of

an identifier, such as a name, an identification number, data of

location, an online identifier or one or more elements of identity

physical, physiological, genetic, mental, economic, cultural or social of said person;

"2) "processing": any operation or set of operations carried out on

personal data or sets of personal data, either by procedures

automated or not, such as the collection, registration, organization, structuring,

conservation, adaptation or modification, extraction, consultation, use,

communication by transmission, diffusion or any other form of authorization of

access, collation or interconnection, limitation, deletion or destruction;

"11) "consent of the interested party": any expression of free, specific,

informed and unequivocal by which the interested party accepts, either through a

declaration or a clear affirmative action, the processing of personal data that

concern".

The denounced facts materialize in the impersonation of the identity of the

claimant by a third party.

From the extract of the indicated card, dated November 2021, by the claimant,

the veracity of the facts claimed is confirmed: two cash withdrawals through

from an ATM in Vigo and two payments in that town.

All this, without your authorization or consent, considering that the

regulations on the protection of personal data.

It should be remembered that to access the telephone service and modify the

associated mobile phone number, the alleged impersonator must know, or the

CAP, or the following personal data of the claimant:

• Full name

• D.N.I. or residence card

• Birthdate

• Full address

• Landline and/or mobile phone

These are data from which it is reasonable to deduce that they can be accessed with

relative ease for potential impersonators.

According to the narrative of the facts verified by the inspection, the impersonator

managed to change the contact telephone number that the claimant had to

disposition of the claimant. With this, there was a treatment without legitimation of the

personal data of the claimant, since his telephone number was suppressed and

simultaneously assigned a new contact telephone number without

consent or legitimizing basis of any of those provided for in article 6.1.

GDPR.

Classification of the infringement of article 6.1 of the GDPR

II

If confirmed, the aforementioned infringement of article 6.1 of the GDPR could lead to the commission of

sion of the offenses typified in article 83.5 of the GDPR that under the rubric

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

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

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

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

overall annual total business of the previous financial year, opting for the one with the highest

amount:

a) the basic principles for the treatment, including the conditions for the consent

lien under articles 5, 6, 7 and 9; (…)”

In this regard, the LOPDGDD, in its article 71 "Infractions" establishes that:

"The acts and behaviors referred to in sections 4,

5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that are contrary to

rias to the present organic law”.

For the purposes of the limitation period, article 72 “Infringements considered very serious”

you see” of the LOPDGDD indicates:

"1. Based on what is established in article 83.5 of Regulation (EU) 2016/679,

are considered very serious and will prescribe after three years the infractions that

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

following:

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

two in article 5 of Regulation (EU) 2016/679. (…)”

Penalty for violation of article 6.1 of the GDPR

IV.

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

In accordance with the evidence available at the present time of

agreement to start disciplinary proceedings, and without prejudice to what results from the

investigation, it is considered that the offense in question is serious for the purposes of the

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

criteria established in article 83.2 of the GDPR:

As aggravating factors:

-

b) The intent or negligence in the offence;

The Supreme Court has understood that imprudence exists 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

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 rigor and exquisite care

for complying with the legal provisions in this regard. [Sentence of the Hearing

National of 10/17/2007 (rec. 63/2006)].

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

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

corrective measures" of the LOPDGDD:

As aggravating factors:

-

of personal data.

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

BANKINTER CONSUMER FINANCE, E.F.C., S.A. is a financial establishment

credit- payment entity.

Consequently and for the purposes of compliance with the legal requirements

established, the exercise of said activity necessarily implies the knowledge and

application of current regulations on the protection of personal data.

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

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

established in article 6.1 of the GDPR, allows the initial setting of a penalty of

€70,000 (SEVENTY THOUSAND EUROS).

V

adoption of measures

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

14/17

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.

Therefore, in accordance with the foregoing, by the Director of the Agency Spanish Data Protection,

HE REMEMBERS:

FIRST: INITIATE SANCTION PROCEDURE against BANKINTER CONSUMER FINANCE E.F.C., S.A., with NIF A82650672, for the alleged violation of Article 6.1 of the GDPR, typified in Article 83.5 of the GDPR.

SECOND: APPOINT as instructor B.B.B. and, as secretary, C.C.C. indicating that may be challenged, where appropriate, in accordance with the provisions of articles 23 and 24 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector (LRJSP).

THIRD: INCORPORATE into the disciplinary file, for evidentiary purposes, the claim filed by the claimant and its documentation, as well as the documents obtained and generated by the Sub-directorate General of Inspection of Data in the actions prior to the start of this sanctioning procedure.

FOURTH: THAT for the purposes provided for in art. 64.2 b) of Law 39/2015, of 1 October, of the Common Administrative Procedure of Public Administrations, the sanction that could correspond would be, for the alleged violation of article 6.1 of the GDPR, typified in article 83.5 of said regulation, administrative fine of amount €70,000 (SEVENTY THOUSAND EUROS).

FIFTH: NOTIFY this agreement to BANKINTER CONSUMER FINANCE E.F.C., S.A., with NIF A82650672, granting it a hearing period of ten days

able to formulate the allegations and present the evidence that it considers

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

procedure that appears in the heading of this document.

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

may be considered a resolution proposal, as established in article

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

Public Administrations (hereinafter, LPACAP).

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

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

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

sanction that should be imposed in this proceeding. With the application of this

reduction, the sanction would be established at 56,000.00 euros, resolving the

procedure with the imposition of this sanction.

In the same way, it may, at any time prior to the resolution of this

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

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

the sanction would be established at 56,000.00 euros and its payment will imply the termination

of the procedure, without prejudice to the imposition of the corresponding measures.

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

apply for acknowledgment of responsibility, provided that this acknowledgment

of the responsibility is revealed within the period granted to formulate

allegations at the opening of the procedure. Voluntary payment of the referred amount in the previous paragraph may be done at any time prior to the resolution. In In this case, if both reductions were to be applied, the amount of the penalty would remain established at 42,000.00 euros.

In any case, the effectiveness of any of the two aforementioned reductions will be conditioned to the withdrawal or resignation of any action or appeal via administrative against the sanction.

In the event that you choose to proceed with the voluntary payment of any of the amounts indicated above (56,000.00 euros or 42,000.00 euros), you must make it effective by entering the account number IBAN: ES00-0000-0000-0000-0000-0000 (BIC/SWIFT Code: CAIXESBBXXX) opened in the name of the Spanish Agency for Protection of Data in the banking entity CAIXABANK, S.A., indicating in the concept the reference number of the procedure that appears in the heading of this document and the reason for the reduction of the amount to which it accepts.

Likewise, you must send proof of income to the General Subdirectorate of Inspection to continue with the procedure in accordance with the quantity entered.

The procedure will have a maximum duration of nine months from the date of the initiation agreement or, where appropriate, of the draft initiation agreement. After this period, its expiration will occur and, consequently, the file of performances; in accordance with the provisions of article 64 of the LOPDGDD.

Finally, it is noted that in accordance with the provisions of article 112.1 of the LPACAP, there is no administrative appeal against this act.

Mar Spain Marti

Director of the Spanish Data Protection Agency

C / Jorge Juan, 6

>>

SECOND: On March 29, 2023, the claimed party has proceeded to pay of the sanction in the amount of 42,000 euros making use of the two reductions provided for in the initiation Agreement transcribed above, which implies the recognition of responsibility.

THIRD: The payment made, within the period granted to formulate allegations to the opening of the procedure, entails the waiver of any action or appeal via against the sanction and acknowledgment of responsibility in relation to the facts referred to in the Commencement Agreement.

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 EXP202202178, in

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

SECOND: NOTIFY this resolution to BANKINTER CONSUMER

FINANCE E.F.C., 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