 File No.: EXP202105689

-

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 23, 2023, the Director of the Spanish Agency for

Data Protection agreed to start a sanctioning procedure against VODAFONE

SPAIN, S.A.U. (hereinafter, the claimed party), through the Agreement that

transcribe:

<<

File No.: EXP202105689

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: Ms. A.A.A. (hereinafter, claimant one) dated October 28,

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

claim is directed against VODAFONE ESPAÑA, S.A.U. with NIF A80907397,

formerly VODAFONE ENABLER ESPAÑA (hereinafter, the claimed party or

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

Claimant one, a user of a mobile telephone line contracted with LOWI, has

been the victim of malicious actions by unknown third parties, consistent

to request a duplicate of your SIM card without your consent, and, after being

granted, make unauthorized transfers of funds from accounts

their banking, contracted with ING and BBVA.

Thanks to the new duplicate, the attacker managed to change the credentials of his box

email at ING, as well as the associated e-mail address. In addition to having

your funds, enabled mobile validation, and added your payment method to Google Pay.

He also changed his AMAZON account credentials, and his email address

linked. The affected party wishes to state that, despite having communicated to LOWI

that she had not requested the duplicate, the operator did not actually block the line, and

it could continue to be used for a while.

Relevant documentation provided by the claimant:

- Document that includes the chronology of events (hereinafter,

“Claimant Chronology”).

Invoice dated September 23, 2021 issued in the name of the claimant

which refers to the number ***PHONE.1 and includes the text “SIM amount: 2.48€;

“SIM discount: - €2.48.

-

-

- Emails received by the claimant at the address ***EMAIL.1 on

September 23, 2021 at 1:30 p.m. from the address ***EMAIL.2 in the

that inform you that they are processing your card duplicate request

SIM (hereinafter, "Claimant Emails").

-

Screenshot of an SMS message (acronym in English for “Short

Message System”, “Short Message System” in Spanish) received on the day

September 23, 2021 at 7:35 p.m. The message indicates that the

sending the requested SIM cards is ready (hereinafter, “SMS

Claimant”).

- Complaint filed by the claimant on September 26, 2021 at

7:35 p.m. before the Mossos d'Esquadra (hereinafter, "Complaint"). Pick up the

chronology of the events, including attempts to impersonate the

identity before ING, BBVA and Amazon.

- Email addressed by the claimant to ***EMAIL.3 on the 28th of

September 2021 to file a claim for the impersonation of

identity and request the cancellation of the line ***TELEPHONE.1. In the writing also

communicates that her telephone number to locate her "now" is

***PHONE.2.

SECOND: Ms. B.B.B. (hereinafter, claimant two) dated May 15,

2022 filed a claim with the Spanish Data Protection Agency. The

claim is directed against VODAFONE ESPAÑA, S.A.U. with NIF A80907397,

formerly VODAFONE ENABLER ESPAÑA (hereinafter, the claimed party or

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

Claimant two states that, on March 1, 2022, she received a call

strange (in which an alleged operator of the claimed party requests your information

bank, without the claimant agreeing to it, hanging up the phone) and a few minutes

later, your mobile phone line (contracted with the claimed party) stops working

function and you cannot access your personal area through the web either.

After contacting your bank, they tell you that a charge had been made on

your bank account, so you request the blocking of your bank account and contact

the claimed party to block your phone line, requesting a new card

SIM (since his was disabled) and upon receiving the SIM (without the delivery person

request any identification document) check that the e-mail address

associated is not yours, so you deduce that a third party accessed your personal area,

modified the contact details and asked the claimed party for a duplicate of his

SIM card, thus being able to access your bank account.

Together with the claim, a screenshot is provided (dated September 25, 2021)

relative to the correct e-mail that was associated with your SIM card, as well as a photograph

certifying that the e-mail associated with the new SIM that you requested was different from the

former.

Likewise, it provides a copy of the complaint filed with the Police (on December 2,

March 2022) and Response of the Respondent (dated April 6, 2022)

regarding the claim presented, which states the following: "Let us

thank you for bringing this situation to our attention... We are sorry

your experience with us very much and we offer you our most sincere apologies

for all the inconvenience caused, we hope that from now on your experience

with Lowi be formidable. Therefore, we consider your claim closed and

We appreciate the trust placed."

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), the claim filed by the claimant was forwarded

one to the claimed party, to proceed with its analysis and inform this

Agency within a month, of the actions carried out to adapt to the

requirements set forth 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) by electronic notification, was not collected by

the person in charge, within the period of availability, understood as rejected

in accordance with the provisions of art. 43.2 of the LPACAP dated January 10, 2022,

as stated in the certificate that is in the file.

Although the notification was validly made by electronic means, assuming that

carried out the procedure in accordance with the provisions of article 41.5 of the LPACAP, under

information, a copy was sent by postal mail, which was duly notified in

dated January 20, 2022. In said notification, he was reminded of his obligation to

interact electronically with the Administration, and were informed of the media

of access to said notifications, reiterating that, in the future, you will be notified

exclusively by electronic means.

On February 10, 2022, this Agency received a written response

indicating

"That a letter has been sent to the claimant through which

proceeded to inform you about the efforts that were carried out by LOWI to

solve the incident and that it is currently resolved. In this

In this sense, attached as Document number 1, a copy of said letter sent to the

claimant, by which he is informed, in particular, that the application for a card

SIM and SIM change have been classified as fraud by the Department of

LOWI fraud.

Likewise, the claimant is informed that the request for a SIM card requested through

of your customer ID was never delivered as it was canceled by LOWI on the 24th of

September 2021.

Therefore, this card could never be activated and this duplicate SIM was never reached.

to run.

Regarding the SIM change that occurred on September 23, 2021, this will be

performed by activating a SIM card previously purchased in a store.

However, on the same day, September 23, LOWI suspended the telephone line of the

claimant to prevent a third party from carrying out any type of action

fraudulent and returned control of its line to the claimant.

Finally, the claimant is informed that she does not have active services available

in LOWI systems.

After analyzing the claim and investigating what happened, LOWI has been able to verify that,

On September 23, 2021, an order for a SIM card was processed at the ID of

AAA customer for the mobile line ***TELEPHONE.1. However, after a

claim submitted by the claimant to the customer service of

LOWI, on September 24, 2021, said order was canceled, which

it was never delivered.

Notwithstanding the foregoing, on the same day, September 23, 2021, LOWI has been able to

confirm that the mobile line ***TELEPHONE.1 of the claimant underwent a SIM change

processed through the call center by activating a purchased SIM card

previously by the impersonator in a store operated by the company

FIBRANORTE, S.L.

Likewise, once the claim from the claimant was received in which she alleged that she had

suffered identity theft and not recognize said change of SIM card, the

Fraud Department proceeded to suspend the affected line, to qualify the

happened as a fraud and to return control over its line to the claimant.

This party wants to point out that my client managed to solve the incidents object

of claim effectively on September 23 and 24, 2021, that is, with

prior to the receipt of this request by the Agency.

Once this claim was received, LOWI verified that what happened had been

classified as a fraud and that control of the affected line was returned to the

claimant on the same day that the SIM card change occurred, that is, on the 23rd of

September 2021. Likewise, it has been verified that the SIM card order that was

made using the claimant's customer ID was canceled on

September 2021 and 3 C2 General never delivered.

However, it has been confirmed that the claimant does not currently have services

in LOWI. All this has been notified to the claimant by sending a letter

which is attached as Document number 1.

In addition, following internal investigations carried out by LOWI, it has been decided

penalize the store that sold the SIM card that was activated by the

alleged impersonator of the claimant's identity.

On the other hand, in order to prevent similar incidents from occurring, LOWI works in

continuously in improving Security Policies for its change processes and

SIM duplicates as well as for any other process that carries potential risks

fraud or irregular actions for our clients.

In this sense, LOWI acts under the Security Policy for the Hiring of

Individuals, which has been progressively updated. Through said Policy

Security, my client establishes what type of information must be required from the

client for each requested management.

Likewise, it is included how to proceed in case a user does not pass the

Security Policy, as well as preventive actions in fraud situations.

The aforementioned Security Policy is mandatory for all

LOWI Post-sale Services, who are in charge of applying and respecting it. In addition,

regarding the processing of a duplicate SIM, in accordance with said

Policies, to make a SIM change by telephone, it is necessary to

performing and exceeding the LOWI Security Policy for such scenarios.

Additionally, it should be noted that all employees in the Department of

Customer Service have received training on the steps to follow to carry out

SIM changes. Therefore, if the processing of a SIM change and/or a change of

ownership exceed the previous LOWI Security Policies, the

carrying out such procedures in accordance with what is indicated in said Policies, when considering

I represented the change as authentic, real and truthful. They are also reviewing

internal processes to ensure compliance with Security Policies

defined or introduce the necessary changes when considered appropriate. In

Specifically, my client is working on the continuous improvement of:

• Review of internal processes to ensure compliance with the Privacy Policies.

Security and verification controls that have been defined and incorporated, both

in face-to-face and telephone channels, for duplicate SIM scenarios.

• Periodic reinforcement of communication of Security Policies and verifications

that have been defined by LOWI for SIM duplicates and that must be

applied by agencies, commercial stores and agents.

• Sending periodic communications to the face-to-face and telephone channel, as well as to the

logistics operator, where it is alerted to the risk scenarios detected, its

characteristics and behavior patterns to prevent new cases. In these

communications include details of how these requests are produced, channels to

through which they are requested, documentation they provide, description of the

handling, geographic areas where the cards are being collected/delivered

Duplicate SIMs.

• Application -if applicable-, of the existing Penalty Policy for agents or

distributors who carry out any duplicate or change of a SIM card without having

required documentation or to carry out any SIM change management without

Follow all the steps defined in the Security Policy. As regards the

carrying out fraudulent banking transactions such as those that

manifested by the claimant in her claim, it is opportune to state that the change

of a SIM card implies only access to the telephone line associated with

this, and not to the bank details of the owner.

Therefore, it does not seem possible that there is a correlation between the events that occurred in

relationship with my client and what happened with the bank of which he is a client

the claimant.

In this sense, the bank movements that you allege in your claim do not have your origin, nor have they been caused by invoices for LOWI services that had contracted, but are due to accesses made through the account of your bank. Therefore, LOWI cannot be responsible for the accesses and bank movements that could have been carried out fraudulently".

FOURTH: In accordance with article 65 of Organic Law 3/2018, of 5 December December, Protection of Personal Data and guarantee of digital rights (LOPDGDD), when submitted to the Spanish Data Protection Agency (hereinafter, AEPD) a claim, it must evaluate its admissibility for processing, must notify the claimant of the decision on the admission or non-admission to procedure, within three months from the date the claim was entered into this Agency. If, after this period, there is no such notification, it will be understood that the processing of the claim continues in accordance with the provisions of Title VIII of the Law. Said provision is also applicable to the procedures that the AEPD would have to process in the exercise of the powers assigned to it attributed by other laws.

In this case, taking into account the foregoing and that the claim is filed with this Agency, on October 28, 2021, it is communicated that with dated January 28, 2022, the claim of claimant one, has been admitted to procedure as three months have elapsed since it entered the AEPD.

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

The claimed party expresses in its writings that there would have been two requests

duplicate SIM card on the claimant's line on the dates indicated

refer. A first request would have been made through the website of the

claimed part, and a second in a physical store.

Responsibility of the claimed party for damages to the claimant

LOWI states that "changing a SIM card only implies access to the

telephone line associated with it, and not to the bank details of the owner". And adds that

"cannot be responsible for the accesses and bank movements that could

have been made fraudulently. Attached is a letter addressed to the claimant on

February 10, 2022 in which he communicates the facts related to the

requests for duplicate SIM cards and expresses that it is not responsible

of banking transactions that may have been carried out fraudulently in

other entities.

About the procedures for requesting and activating duplicate SIM cards

The Respondent has provided a document that includes a chart describing the

SIM card change process. The graph shows two possible itineraries: one,

when the request is made through a distributor; other, when it starts

by telephone (through the number "121") or from the "private area" of the client.

According to the information consulted, "121" is the telephone number for customer service.

client of the defendant.

In relation to the request initiated by the distributor, the defendant describes the process

in the following terms:

(…)

In relation to the request initiated by telephone (through "121") or from the

client's private area (internet), specify the following steps:

(…)

In addition, LOWI declares that it has a Security Policy for the

Hiring of Individuals that establishes what type of information must be required from the

client for each management requested in order to avoid fraud. Add that moves to

customer service providers (refers to “Majorel”) the process for

process SIM change requests. This document includes the following

Steps:

(…)

The claimed party also states that the employees of the Customer Service

Customer receive training on what type of information should be required for each

management, including SIM card activation request.

On the first request made on behalf of the claimant

From the documentation collected, the following chronology of events in

in relation to the first request for a duplicate SIM card:

- The claimed party states that on September 22, 2021 at 8:56 p.m.

hours a person contacted their customer service who provided

the data of the claimant to request information on how to request a

duplicate SIM card. In this regard, the defendant has provided:

o Screenshot of the information systems of the party

claimed that references the record of an incoming call to attention

to the customer on September 22, 2021 at 8:56 p.m. in

relation to the number of the claimant.

o Audio recording: the caller provides the full name and the

ID number of the claimant to identify himself. The agent provides

information on the different channels for requesting duplicates

of SIM cards: “Media Markt” store (with activation of the card in the

own store -says the agent who for two months has not been

allows telephone activation-); by phone (with delivery to the address

that is consigned in the system - refers to the agent who cannot

change address-); or through the application with delivery to the

address chosen.

- The claimed party states that on September 23, 2021 at 1:30 p.m.

hours a person requests through the customer area of the website of the

claimed a change of the SIM card for the number of the claimant.

It states that in order to access the customer area it is necessary to facilitate the

customer's phone number or email and password

access. It states that the person knew said data because he agreed and requested

the duplicate. LOWI expresses that the SIM cards requested through this

procedure are sent inactive to the address provided by the interested parties and

that it is the receiver who has to activate them once they receive them. The part

claimed has provided:

o Screenshot of the internet page for access to the area of

customers of the claimed party in which it is observed that two

data to access: email or phone number, and a

access password.

o The data of the request for a duplicate SIM card made on the day

September 23, 2021 at 1:30 p.m. through the “WEB” channel.

The shipping address is not listed.

- The claimed party states that on September 23, 2021 at 1:30 p.m.

sent two emails to the claimant in which they informed her that

they were processing your duplicate request. One of them contains the text

"Remember to have your ID on hand to be able to pick it up." These emails

emails match those provided by the claimant (Emails

complainant)

- The claimed party states that the notification of the sending of a new

SIM card is also done via SMS text message. so attached

a screenshot showing the message sent on the 23rd of

September 2021 at 7:35 p.m. with the text “SIM cards are already

ready for shipment. You will receive it shortly at the address you indicated.

This message coincides with the one provided by the claimant (SMS Claimant).

- The claimed party states that, once the previous communications

make the claimant aware of the situation, call the customer service

to the client.

The claimed party has provided:

-

o An audio recording (“SECOND CALL CD” attached to the

Writ #3) in which the calling party states that they have received a

text message (SMS) informing you of the shipment of SIM cards and indicates

that he has stopped having a line in his terminal. Provide ID, name and

Surname of the claimant, and telephone number ***TELEPHONE.1.

He states that he has not contacted the defendant during the

day to carry out any procedure. The agent explains that previously

have called requesting information on how to request a duplicate of

SIM card and that someone, posing as it, has managed to

Activate a store-bought SIM card. Express what proceeds

then to block the line and establish a “security word”

for communications between the complainant and the defendant.

- It also expresses the claimed party that proceeded to block the shipment of the

duplicate SIM card requested through the customer area of the

claimant. In this regard, the defendant also states that "it was sent

communication via email to logistics to proceed to the

cancellation of the sending of the request made by the offender by the page

Web".

In this regard, the defendant has provided:

o Information from the system registry of the claimant on the 23rd of

September 2021 at 9:55 p.m. that refers to the sending of an email

email "to o2o to cancel duplicate sim card".

o Screenshot of the claimant's information systems in the

containing information on the shipment addressed to the claimant with

indication of the destination address. Includes registration of the request

return to the transport company by order of the person claimed on the day

September 24, 2021 at 9:24 a.m., as well as the execution of

return to origin.

The claimed party states that this first request for a duplicate could be made

of the SIM card through its website because the applicant had

knowledge of the data necessary to access the client area of the claimant.

Regarding the second request made on behalf of the claimant

The claimed party states that through this second request the

activation of a SIM card purchased in a physical store operated by the company

FIBRANORTE, S.L.

The Respondent provides the following chronology of facts in relation to this

second request:

- In their information systems there are several calls received on the 23rd of

September 2021 by the claimed party associated with the claimant.

o The first record, at 1:42 p.m., refers to the call of an installer

of the defendant requesting information about a SIM card. According to

Registered information is referred to customer service.

o The second record, at 1:57 p.m., refers to a call in which

Activation of a store-bought SIM card is requested. Is according

specifies, it is reported that this procedure is not carried out by telephone.

Attaches an audio recording in which the caller facilitates the
ID number of the claimant to identify herself and states that she is
in a store and that you have purchased a SIM card. This person requests
that they modify the "ICC" in their record for the number ***TELEPHONE.1 to
in order to activate the new card. The operator tells you that they have you
to activate the SIM card in the store because they do not activate by phone
cards purchased in store.

o The third record, at 2:07 p.m., refers to an outgoing call from the
“Click2Call” channel. It refers that a duplicate SIM card is requested in
a store and you are informed that you cannot modify the "ICC" of a
"high in store".

o The fourth record, at 6:00 p.m., refers to an incoming call on the
that the caller “seeks a Vodafone store for a duplicate”.

Attaches an audio recording in which the caller facilitates the
DNI number and the name and surname of the claimant to
identify. Request the address of a physical store in which to make a
duplicate SIM card. The agent gives you the address of a
physical store where the duplicate will be processed.

Also, attach an audio recording in which the caller
He states that he has lost the SIM card and wants a duplicate. request the
Address of a physical store in which to carry out the procedure. The agent
It provides several addresses of physical stores in which to process it.

- On September 23, 2021 at 6:43 p.m., the registration of the party
claimed picks up another incoming call in which information is consulted

on duplicate and you are informed. About this call manifests the party

claimed that in this interaction the agent, skipping the procedure,

executed SIM change activation. It also states that "it has proceeded to

penalize the agency, as a tool to reinforce the obligation of the

monitoring of policies and procedures".

- As seen in the previous section referring to the first application, the day

September 23, 2021 at 7:35 p.m. the claimed party sends a

text message (SMS) informing the claimant of the processing of the

duplicate of the SIM card that is "ready for shipment".

- Expresses the claimed party that as a consequence of the activation of the

duplicate, the claimant lost service on her own phone. In addition,

the Claimant Chronology states that on September 23, 2021 at

20:01 he ran out of phone line on his phone, which shows him the message

"SIM has not been provisioned".

- On September 23, 2021 at 8:31 p.m., the registration of the party

Claimed picks up an incoming call on which it is noted that "they are

impersonating the identity and requesting a duplicate in his name... blocks the

line". Likewise, the record includes a management carried out at 8:34 p.m. in

which establishes the "temporary suspension" of the line.

Attach an audio recording ("SECOND CALL CD") in which the

caller declares that he has received a text message informing him

that they are going to send you a SIM card that you have not requested. It also indicates that he has stopped having a line in his terminal. The caller provides the ID, name and surname of the claimant, and the telephone number ***TELEPHONE.1. He also states that during today he has not contacted the claimed part. The agent explains that they have previously called requesting information on how to request a duplicate SIM card and that someone, posing as the claimant, has managed to activate a card SIM purchased in store. It then proceeds to block the line and establish a "security word" for communications between the complainant and the party claimed.

The claimed party states that at that time it blocked the SIM card.

After this, the Complainant Chronology details information on the following events

- On September 24, 2021 at 09:36 a.m., the registration of the party claimed contains information about an incoming call made from the number ***TELEPHONE.2 (the one that the claimant refers to as her new number) requesting the temporary deactivation of the line ***TELEPHONE.1.

- On September 26, 2021 at 2:29 p.m., the Complainant Chronology refers that the claimant called the usurped telephone number and "gives a line with announcement at the end that this user has unsubscribed the line".

- On September 26, 2021 at 2:43 p.m., the record of the claimed picks up an incoming call made from the number ***PHONE.2 that refers to a query about the number ***TELEPHONE.1 that "yesterday" came out off and "today" with "restricted calls".

- On September 26, 2021 at 5:15 p.m., the Claimant Chronology refers to who filed a complaint about these events with the Mossos d'Esquadra.

- The claimant's record contains subsequent interactions in which

quotes the cancellation of the services contracted by the claimant with the claimant and the

filing of an official claim for identity theft.

On the implications of the blockade of the line

The defendant states that after the blocking of the telephone line, its activity

“it is reduced to the mere reception of calls”. In this regard, provide a copy

of the invoice issued in the name of the claimant for the month of September 2021

which includes the list of outgoing calls made from the number

***TELEPHONE 1. The list does not contain calls made after the 23rd

of September. In addition, it only records a call made on the 23rd of

September, at 7:58 p.m., to the number ***TELEFONO.3. the annex

provided by the claimant states that the supplanter at that time made a

outgoing phone call from your line ***TELEPHONE.1 and in the Express Complaint

that the call was made to the ING bank.

CONCLUSIONS

Previous investigation actions initiated as a result of the receipt of a

claim in which the claimant states that in the month of September 2021

a third party impersonated the claimed party and obtained a SIM card

associated with your phone number.

From the information gathered during the investigation, it has been revealed that

on September 22 and 23, 2021, a person who identified himself with the

name, surnames and ID number of the claimant requested by telephone the
requested information on the ways to request a duplicate of your SIM card.
Subsequently, on September 23, 2021, on behalf of the claimant,
two processes for changing the SIM card associated with your phone number.
The claimed party has provided the protocols available for the replacement of the
SIM cards. However, the information obtained shows that after several attempts the
applicant was able to obtain the duplicate without fully applying the
protocol.
The first of the processes to obtain a duplicate SIM card was carried out through
from your customer account (user area) on the website of the defendant. This
The request could have been made since, according to what the defendant stated, the
applicant had the means of access (username and password) to access the
Claimant's customer area. As part of the process, the claimed party directed
various email and SMS communications with status information
of the physical shipment of the new SIM card. The claimant, after receiving the SMS, contacted
with the requested party in order to inform that she had not made such a request.
This first request concluded with the cancellation of the request (from the evidence
obtained, it can be deduced that the duplicate SIM card was not sent to the
addressee).
The second of them was carried out by telephone activation of a SIM card
previously purchased in person at a store. As stated by the
claimed party, the process of acquiring a duplicate SIM at a distributor
implies the identification of the applicant through his ID (of which the distributor must
keep record). It has also indicated that the protocol provides that the cards
SIMs purchased through this route must also be activated from the SIM itself.
store, without this being able to be done by the user himself through the internet or

by phone. The claimed party states that, on this occasion, by mistake and after

After several attempts by the applicant, an agent activated the store-bought SIM card at the

course of a call from the applicant to customer service. The activation of

the new SIM card caused the claimant to no longer have the line in her

own device. This, and the prior receipt of the text message (SMS) reviewed

previously, had the claimant contact the service of

customer service of the claimed party in order to communicate the facts. During the

call indicates that the fraudulent duplicate of the card is blocked

SIM and the establishment of a security word as an additional security measure.

identification in communications between the claimant and the respondent. Manifests the

claimed that the blocking of the telephone line reduced its activity “to the mere

Receiving Calls". The measure taken at this first moment, therefore, does not

would have contemplated the complete disabling of the line in the duplicate of the card

SIM. Subsequently, the claimant first requested the deactivation of the

line, and subsequently the cancellation of the services contracted with the claimed party.

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

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

forward LOPDGDD), the claim filed by the claimant was forwarded

two to the claimed party, to proceed with its analysis and inform this

Agency within a month, of the actions carried out to adapt to the

requirements set forth 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) by means of electronic notification, was collected by the responsible June 13, 2022, as stated in the acknowledgment of receipt that works in the proceedings.

"On July 27, 2022, this Agency received a written response indicating

After carrying out the appropriate investigations into what happened and having confirmed my represented that all the pertinent actions have been carried out previously

Upon notification of this request for information, a letter has been sent letter to the claimant informing her about the steps that were taken carried out by LOWI to solve the incident and that it is currently resolved.

In this sense, attached as Document number 1, a copy of said letter sent to the claimant, by means of which transfer is given, in particular, of the policies of security available to LOWI to prevent the making of duplicates of SIM card and that what happened has been classified as fraud by the LOWI Fraud Department.

In addition, it is reported that the claimant regained full control over the line ***TELEPHONE.4 affected on March 1, on the very day on which he posted the facts to the knowledge of LOWI.

Finally, it is indicated that the delivery of the new SIM card was made at home confirmed by the claimant herself during the processing of the duplicate.

The claim originates from the fact that the claimant, a user of the telephone line cell phone ***TELEPHONE.4 contracted with my client LOWI, alleges in his claim having been the victim of malicious actions by an unknown third party

by means of which the email address associated with the client ID would have been modified,

would have requested a duplicate of his SIM card without his consent and, after being

granted, non-consented operations would have been carried out through your account

banking.

After analyzing the claim and investigating what happened, LOWI has been able to verify that,

on March 1, 2022, a duplicate SIM not recognized by the

claimant on the line ***TELEPHONE.4 associated with the claimant's customer ID.

To do this, the person who contacted LOWI customer service, after

provide the data that was requested and exceed the LOWI Security Policy,

made a change to the email address associated with the phone line and,

finally, a SIM change at 1:59 p.m.

Subsequently, through two calls from the telephone lines

***TELEPHONE.5 and ***TELEPHONE.6, in which the Security Policy of

LOWI, the claimant indicated that she had suffered an identity theft and denounced a

possible duplicate SIM, having lost access to the LOWI network and access to the

customer.

For this reason, on March 1, the LOWI customer service

proceeded to suspend the affected line, qualifying what happened as a fraud and

return control over its line to the claimant, processing a new duplicate of

SIM, sent to the postal address confirmed by the claimant.

This part wants to point out that the effective management of a change of SIM card, either

requested in a physical store or by telephone, entails overcoming the policies
security that LOWI has implemented in order to prevent them from being carried out
fraudulent practices on the personal data of its clients.

In this sense, and having processed said management subject to said privacy policy,
security, my client understood at all times that they were dealings
lawful, real and truthful. However, in view of the events that occurred, when the
claimant transfers the loss of network and access to its customer area, indicating that
does not recognize the associated email address as its own, my represented
proceeded to carry out the appropriate investigations and procedures in order to resolve the
incident occurred and make a new SIM change that would return control to the
claimant on the line.

Thus, the same day that the facts that are the subject of the claim were confirmed, after
verify LOWI that it was dealing with actions that, despite having the appearance of being truthful,
were of a fraudulent nature, just a matter of a couple of hours my represented
proceeded to block the customer's SIM card to prevent future attacks,
control of their SIM card was returned to the claimant and a new duplicate was processed
SIM.

Thus, the claimant regained control over her telephone line in the same
day on which the duplicate not recognized by the claimant was produced. In
In parallel, the Fraud Department proceeded to classify what happened as a fraud
and, consequently, the fraud victim check was activated in the customer ID of the
claimant.

Therefore, my client managed to solve the incident that is the object of the claim of
effective on March 1, 2022, that is, the same day on which the
produced the fraudulent events and prior to the receipt of this
requirement by the Agency.

Despite taking the above steps, the claimant proceeded to file

a complaint to the police, dated March 2, 2022, a claim to the

LOWI customer service, as well as file a claim with

this Agency, with registration date May 15, 2022, which has resulted in the

present request for information.

Once this claim was received, LOWI verified that what happened had been

classified as a fraud and that the affected line was under the ownership of

the claimant. Likewise, my client included the personal data of the claimant

in LOWI's fraud prevention files to prevent it from being reintroduced.

produce a similar situation in the future. All this has been notified to the claimant

by sending a letter attached as Document number 1.

Regarding the telephone call initially received by the complainant, my principal

has been able to verify, after carrying out the appropriate investigations, that the line

***TELEPHONE.7, from which the claimant denounces having been

contacted by telephone under the argument of acting as operator of LOWI and

there is an incident with a charge on your bank account, it is not linked to LOWI,

nor does it appear in the distribution databases of this entity, nor does it exist

Evidence that none of your agents or collaborators have made the call

indicated.

Likewise, it is interesting to point out that, in accordance with its internal policies, my

client never requires account numbers or billing information over the phone

or by email.

Thus, we understand that it is outside the scope of responsibility of my

principal the personal information that could have been shared through this

type of fraudulent actions, since the interested parties also have the

responsibility to duly safeguard your personal data, being only

within the sphere of control of my client the adequate definition of the

procedures, systems, controls and security measures applicable based on

The criticality of the treatment that ensures the correct identification of the owner of the data.

personal information.

On the other hand, in order to prevent similar incidents from occurring, LOWI works in

continuously in improving Security Policies for its change processes and

SIM duplicates, as well as for any other process that entails possible

risks of fraud or irregular actions for our clients. In this sense,

LOWI acts under the Security Policy for the Hiring of Individuals, which

It has been progressively updated.

Through said Security Policy, my client establishes what type of

information must be required from the client for each requested management. Also, it remains

including how to proceed in case a user does not pass the Security Policy,

as well as preventive actions in fraud situations. The aforementioned

Security Policy is mandatory for all employees of

LOWI, who are in charge of applying and respecting it. Attached as Document

number 2 copy of LOWI's Personal Security Policy.

Consequently, if the processing of a SIM change and/or a change of ownership

exceed the aforementioned LOWI Security Policies, the

carrying out such procedures in accordance with what is indicated in said Policies, when considering

I represented the change as authentic, real and truthful.

On the other hand, with regard to carrying out banking transactions of

fraudulent nature such as those revealed by the claimant in her

claim, it is opportune to express that the change of a SIM card implies

only access to the telephone line associated with it, and not to the data

owner's bank Therefore, it does not seem possible that there is a correlation between the

events that occurred in relation to my client and what happened with the bank

of which Mrs. Soto is a client. In this sense, the bank movements that

alleges in his claim do not have their origin, nor have they been caused by

invoices for LOWI services that he had contracted, but are due to accesses

made through your bank account. Therefore, LOWI cannot be

responsible for the accesses and bank movements that could have been made

fraudulently.

Lastly, regarding the delivery of the new SIM card to the address of the

claimant, it is necessary to clarify that the claimant confirmed by telephone, after

exceed LOWI's Security Policy, the mailing address for sending this

card, which was received without any incident, as recognized in the card itself

claim.

With all this, we can confirm that currently my client has carried out

all pertinent actions to resolve the claim, estimating that

has been correctly resolved prior to the receipt of this

written".

SEVENTH: In accordance with article 65 of Organic Law 3/2018, of 5 December, Protection of Personal Data and guarantee of digital rights (LOPDGDD), when submitted to the Spanish Data Protection Agency (hereinafter, AEPD) a claim, it must evaluate its admissibility for processing, must notify the claimant of the decision on the admission or non-admission to procedure, within three months from the date the claim was entered into this Agency. If, after this period, there is no such notification, it will be understood that the processing of the claim continues in accordance with the provisions of Title VIII of the Law. Said provision is also applicable to the procedures that the AEPD would have to process in the exercise of the powers assigned to it attributed by other laws.

In this case, taking into account the foregoing and that the claim is filed with this Agency, on October 28, 2021, it is communicated that with dated August 15, 2022, the claim of claimant two has been admitted to procedure as three months have elapsed since it entered the AEPD.

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: "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

In advance, it is necessary to point out that article 4.1 of the GDPR defines: "personal data" as "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;"

In this regard, it should be clarified that the card is inserted inside the mobile terminal. SIM. It is a smart card, in physical format and small in size, which contains a chip in which the service key of the subscriber or subscriber is stored used to identify itself to the network, that is, the mobile telephone line number of the MSISDN client (Mobile Station Integrated Services Digital Network - Mobile Station of the Integrated Services Digital Network-), as well as the personal identification number IMSI (International Mobile Subscriber Identity) subscriber Mobile Subscriber-) but can also provide other types of data such as the

information about the telephone list or the calls and messages list.

On the other hand, the issuance of a duplicate SIM card supposes the treatment of the

personal data of its owner since it will be considered an identifiable natural person any

person whose identity can be determined, directly or indirectly, in particular

by means of an identifier (article 4.1) of the GDPR).

Therefore, the SIM card identifies a telephone number and this number in turn,

identifies its owner. In this sense, the CJEU Judgment in case C -

101/2001 (Lindqvist) of 6.11.2003, paragraph 24, Rec. 2003 p. I-12971: "The concept of

"personal data" using Article 3(1) of Directive 95/46

includes, according to the definition in Article 2(a) of said

Directive "all information about an identified or identifiable natural person". This

concept includes, without a doubt, the name of a person next to his telephone number or

to other information relating to their working conditions or hobbies".

In short, both the data processed to issue a duplicate SIM card and the

SIM card (Subscriber Identity Module) that uniquely identifies

to the subscriber in the network, are personal data, and their treatment must be

data.

subject

protection

normative

of

of

the

to

Well then, the defendant is accused of committing an offense for violation of the

Article 6 of the GDPR, "Legacy of the treatment", which indicates in its section 1 the

cases in which the processing of third-party data is considered lawful:

"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.

application to processing carried out by public authorities in the exercise of their

functions".

II

Classification and classification of the offense

The infringement is typified in article 83.5 of the GDPR, which considers as such:

"5. Violations of the following provisions will be penalized, in accordance with the

section 2, with administrative fines of a maximum of 20,000,000 EUR or,

in the case of a company, 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:

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

consent in accordance with articles 5,6,7 and 9."

The LOPDGD, for the purposes of the prescription of the infringement, qualifies in its article 72.1

very serious infringement, in this case the limitation period is three years, "b)

The processing of personal data without the fulfillment of any of the conditions of

legality of the treatment established in article 6 of Regulation (EU) 2016/679".

In the present case, it is proven that LOWI provided a duplicate of the card

SIM of the claimant one and two to a third party, without their consent and without verifying the

identity of said third party, which has accessed information contained in the phone

mobile, such as bank details, passwords, email address and others

personal data associated with the terminal. Thus, the defendant did not verify the

personality of the person who requested the duplicate SIM card, did not take precautions

necessary for these events not to occur.

Based on the foregoing, in the case analyzed, the

diligence used by the defendant to identify the person who requested

a duplicate SIM card.

Well, according to what the defendant stated, "LOWI has been able to confirm that

the mobile line ***TELEPHONE.1 of claimant one underwent a SIM change processed to

through the call center by activating a purchased SIM card

previously by the impersonator in a store operated by the company

FIBRANORTE, S.L.

On the other hand, LOWI points out in relation to the claimant that, on this occasion,

by mistake and after several attempts by the applicant, an agent activated the purchased SIM card

in store in the course of a call from the applicant to customer service.

The activation of the new SIM card caused claimant one to stop

have the line on your own device.

On the other hand, in relation to the claimant two LOWI states, "After analyzing the

claim and investigate what happened, LOWI has been able to verify that, on

March 2022, a duplicate SIM not recognized by the claimant was processed two

on the line ***PHONE.4 associated with the customer ID of claimant two. For

Therefore, the person who contacted LOWI customer service, after

provide the data that was requested and exceed the LOWI Security Policy,

made a change to the email address associated with the phone line and,

finally, a SIM change at 1:59 p.m.

However, it should be noted that Sim Swapping is a fraud that allows you to impersonate

identity by kidnapping the phone number by obtaining a duplicate of

the SIM card.

In any case, the operator must be able to prove that for this specific case

have followed the verification protocols implemented when requesting a

duplicate SIM card.

Well then, the result was that the defendant issued the SIM cards to a third party who

he was not the owner of the line.

In view of the foregoing, the claimed party fails to prove that this

procedure.

In the explanation provided by the claimed party, it does not indicate which could have

been the specific cause that led to the issuance of duplicates, beyond

some generic explanations about a possible “human error”, non-compliance by the

LOWI collaborators, or even “organized criminal activity”. In any case, the

The claimed party has not been able to prove that, for this case, the

procedure implanted by herself, since, if she had done so, she should have

The refusal of the duplicate of the SIM card occurred.

Based on the foregoing, in the case analyzed, the

diligence used by the defendant to identify the person who requested

a duplicate SIM card.

In accordance with the evidence available at this procedural moment and

without prejudice to what results from the investigation of the procedure, it is estimated that the

conduct of the claimed party could violate article 6.1 of the GDPR and may be

constituting the offense classified in article 83.5.a) of the aforementioned Regulation

2016/679.

In this sense, Recital 40 of the GDPR states:

"(40) For processing to be lawful, personal data must be processed with the

consent of the interested party or on some other legitimate basis established in accordance

a Law, either in this Regulation or under other Union law

or of the Member States referred to in this Regulation, including the

the need to comply with the legal obligation applicable to the data controller or the

need to execute a contract to which the interested party is a party or for the purpose of

take measures at the request of the interested party prior to the conclusion of a

contract."

IV.

Sanction proposal

The determination of the sanction that should be imposed in the present case requires

observe the provisions of articles 83.1 and 2 of the GDPR, precepts that,

respectively, provide the following:

"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, 9 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, in addition to or in lieu of 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

such as the number of interested parties affected and the level of damages that

have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the person in charge or in charge of the treatment to

settle the damages suffered by the interested parties;

d) the degree of responsibility of the person in charge or of the person in charge of the treatment, habi-

gives an account of the technical or organizational measures that have been applied by virtue of the

articles 25 and 32;

e) any previous infringement committed by the controller or processor;

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

infringement and mitigate the possible adverse effects of the infringement;

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

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

particular whether the person in charge or the person in charge notified the infringement and, if so, in what

extent;

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

previously against the person in charge or the person in charge in relation to the

same matter, compliance with said measures;

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

fications approved in accordance with article 42, and

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

as the financial benefits obtained or the losses avoided, directly or indirectly.

mind, through infraction."

Within this section, the LOPDGDD contemplates in its article 76, entitled "Sancio-

and corrective measures":

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

(UE) 2016/679 will be applied taking into account the graduation criteria

established in section 2 of said article.

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

may also be taken into account:

a) The continuing nature of the offence.

b) The link between the activity of the offender and the performance of data processing.

personal information.

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 by absorption process subsequent to the commission of the

violation, 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.

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

alternative conflict resolution mechanisms, in those cases in which

there are controversies between those and any interested party.

3. It will be possible, complementary or alternatively, the adoption, when appropriate, of

the remaining corrective measures referred to in article 83.2 of the Regulation

(EU) 2016/679."

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 on the entity claimed as responsible for an infringement classified in the article 83.5.a) of the GDPR and 72.1 b) of the LOPDGDD, in an initial assessment, The following factors are considered concurrent in this case:

As aggravating factors:

-

The evident link between the business activity of the defendant and the treatment of personal data of clients or third parties (article 83.2.k, of the GDPR in relation to article 76.2.b, of the LOPDGDD).

No. of interested parties affected: The initiation agreement includes the claims made by two claimants.

The Judgment of the National Court of 10/17/2007 (rec. 63/2006), in which, with respect to entities whose activity entails the continuous processing of customer data, indicates that "...the Supreme Court has understood that recklessness exists whenever a legal duty of care is neglected, that is that is, when the offender does not behave with the required diligence. And in the assessment of the degree of diligence, special consideration must be given to the professionalism or not of the subject, and there is no doubt that, in the case now examined, when the appellant's activity is constant and abundant handling of personal data must insist on rigor and exquisite Be careful to comply with the legal provisions in this regard."

As mitigations:

The claimed party proceeded to resolve the incident that is the object of the claims of

effective form (art. 83.2 c).

It is appropriate to graduate the sanction to be imposed on the defendant and set it at the amount of one hundred

€40,000 for the alleged infringement of article 6.1) typified in article

83.5.a) of the aforementioned GDPR.

Therefore, in accordance with the foregoing, by the Director of the Agency

Spanish Data Protection.

HE REMEMBERS:

FIRST: INITIATE SANCTION PROCEDURE against VODAFONE SPAIN,

S.A.U. with NIF A80907397, formerly VODAFONE ENABLER ESPAÑA (LOWI)

for the alleged violation of article 6.1) typified in article 83.5.a) of the aforementioned

GDPR.

SECOND: APPOINT as instructor D. R.R.R. and as secretary to Mrs. S.S.S.,

indicating that any of them may be challenged, if applicable, in accordance with the provisions

established in articles 23 and 24 of Law 40/2015, of October 1, on the Legal Regime

co of the Public Sector (LRJSP).

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

claim filed by the claimant and its documentation, the documents

obtained and generated by the General Subdirectorate of Data Inspection.

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 infringement of article 6.1 of the GDPR,

typified in article 83.5 a) of the GDPR, the sanction that would correspond would be a

a fine of 140,000 euros (one hundred and forty thousand euros) without prejudice to the

resulting from the instruction.

FIFTH: NOTIFY this agreement to VODAFONE ESPAÑA, S.A.U. with NIF

A80907397 granting a hearing period of ten business days to formulate

the allegations and present the evidence it deems appropriate. In his writing of

allegations must provide your NIF and the procedure number 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, in the event that the

sanction to be imposed other than a fine, may recognize its responsibility within the

term granted for the formulation of allegations to the present initiation agreement; it

which will entail a reduction of 20% for the sanction that should be imposed

in this proceeding, equivalent in this case to twenty-eight thousand euros (28,000

€). With the application of this reduction, the amount of the sanction would be established in

one hundred and twelve thousand euros (€112,000), resolving the procedure with the imposition of

this sanction, without prejudice to the imposition of corrective measures that, where appropriate,

can correspond.

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, in

accordance with the provisions of article 85.2 LPACAP, which will mean a

reduction of 20% of the amount of the same, equivalent in this case to twenty-eight

thousand euros (€28,000), for the infringement charged. With the application of this reduction, the

amount of the sanction would be established at one hundred and twelve thousand euros (€112,000) and its

payment will imply the termination of the procedure, without prejudice to the imposition of the

corrective measures that, where appropriate, may correspond.

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 eighty-four thousand euros (€84,000).

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, 112,000 euros or 84,000 euros, you must make it effective

by depositing it in the account number ES00 0000 0000 0000 0000 0000 opened to

name of the Spanish Data Protection Agency at CAIXABANK Bank,

S.A., indicating in the concept the reference number of the procedure that appears in

the heading of this document and the reason for reducing the amount to which

welcomes.

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

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

25/26

SECOND: On February 15, 2023, the claimed party has proceeded to pay

of the sanction in the amount of 112,000 euros using one of the two

reductions provided for in the Commencement Agreement transcribed above. Therefore, there has not

The acknowledgment of responsibility has been accredited.

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

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 EXP202105689, in

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

SECOND: NOTIFY this resolution to VODAFONE ESPAÑA, S.A.U..

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

937-181022

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es