Procedure No.: PS/00001/2021

RESOLUTION OF PUNISHMENT PROCEDURE

Of the procedure instructed by the Spanish Agency for Data Protection (as regards

hereafter, AEPD) and based on the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the claimant party one), on September 2

2019, files a claim with the AEPD against VODAFONE

SPAIN, S.A.U. with CIF A80907397 (hereinafter, VODAFONE or VDF), for the

following reasons:

“On August 5, around 9:00 p.m. at night, I verify that my terminal

terminal with your company's line ***TELEPHONE.1 is left without the network and

I can't make or receive calls, so I call Customer Service.

Customer and after 2 minutes of waiting they tell me that the line is fine and that they come

give it to a Distributor (Vodafone store) to see if you can try any

problem in the SIM card, which may be damaged and that is solved with

a change of it.

The next day, August 6, since I work in a town 70 kms

from my home and there is no store there, I can't do it until 6:30 p.m.

in the afternoon and I go to the Vodafone store on Calle Ancha

nº 26 where in addition to providing me with a new SIM at a cost of 5 euros, I

they contract an offer of some more channels to my TV from the package that I have

hired.

At the time of recovering the phone, around 7:04 p.m. and once

my line is established normally, I receive input of new messages and in

one of them, an Alert from Banco de Santander, tells me that I am realizing-

I make a transfer from my online banking and, if not, put me

contact the ***TELEPHONE number from 9:00 a.m. to 7:00 p.m.

which I do not do, because I receive it at 7:04 p.m.

When I arrive at my home, I try to enter Digital Banking but I cannot access

der with my passwords to check if there has been any movement ex-

strange in my account, which I postpone for the next day August 7 in the

Banco de Santander branch in ***LOCALIDAD.1, place where I work;

It is at the branch when an employee takes an extract from me where I communicate

nican that I have granted and contracted a Loan, and once granted

there have been 25 expense operations, credit card purchases, transfers,

references, and payments to other entities, which I have not made, so I go

to file a complaint with the Civil Guard, because some person or person

sonas, has used my passwords and my access to Banca On Line del San-

tander, to do all those operations fraudulently.

It's obvious they used my hijacked phone line for a day and a half,

date on which I go to personally make a duplicate of my card.

After the Complaint, and in a call to Vodafone asking me about what

what had happened in those two days, an agent of the Company informed me

ma that on the 5th at 8:39 p.m., some person or persons,

They made a duplicate of my card at the Vodafone Store in the Centro Co-

commercial "***CENTRO.1" of ***LOCALIDAD.3 (Cornellá) that I have not done-

do and therefore I REPORT for identity theft, or negligence

who or who allowed that change with my data, while I was 800

km away.

This causes the subsequent crime or crimes of fraud, entering into a contract

irregular of a Loan in my name and the purchase of credit cards with

balances, in addition to insurance and various movements with that money obtained

do, which I have not authorized."

Together with the claim, it provides the complaint filed with the Civil Guard of

LOCALIDAD.1 (PROVINCIA.1), on August 7, 2019, with identification number

certified ***ATESTADO.1` and the invoice number ***FACTURA.1 issued by VDF in

that same date, which contains the charge corresponding to the issuance of a card

SIM ((Subscriber Identity Module), where

specifies as delivery address a Shopping Center located in the municipality of

*** LOCATION.2, when CLAIMANT ONE has his habitual residence in the

municipality of *** PROVINCE.1.

In accordance with the provisions of article 65.4 of Organic Law 3/2018, of December 5,

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

hereafter, LOPDGDD), which consists of transferring them to the Delegates of

Data Protection designated by those responsible or in charge of the treatment, or

to these when they have not been appointed, and with the purpose indicated in the aforementioned

article, on October 21, 2019, the claim was transferred to VDF,

to proceed with its analysis and provide a response within a month.

In response to said request, VDF states -among other arguments- the following:

following:

"After analyzing the complaint filed by Mr. A.A.A. and carry out the investigations

timely internal investigations, we have verified that on August 5,

2019, a SIM card change is made at the Vodafone Store located at

the ***CENTRO.1 Shopping Center, for the ***TELEPHONE.1 line associated with

D. A.A.A., residing at C/ ***DIRECTORY.1, ***PROVINCE.1.

In his complaint, Mr. A.A.A. states that, on August 7,

2019, he went to the Civil Guard of ***LOCALIDAD.1 (***PROVINCIA.1) de-

announcing the possibility that his identity had been supplanted and

made a duplicate of your SIM card without your consent, associa-

delo to a series of banking operations carried out in his name with a

unrecognized bank loan from Banco Santander. The next day re-

sends a letter by email to my represented, about the same

facts.

By conducting the appropriate internal investigations into the duplication of

SIM card that is claimed, Vodafone proceeded to (...).

Likewise, and in accordance with Vodafone's security policy, the

The issuance of a duplicate SIM card can only be processed if (...).

Vodafone's security policies are made available to everyone

our collaborators and suppliers, being the fulfillment of their dispositions

mandatory for all its employees. However, there may be

sos in the aforementioned third parties, for reasons unrelated to

Vodafone and outside its control since they are the result of decision-making

sions of a person, do not comply with all of the provisions of said

politics.

In any case, Vodafone proceeded to take the necessary actions

sarias to ensure the security of the account. For this purpose, the SIM card

duplicate object of claim has been duly blocked.

Notwithstanding the foregoing, from my client it has not been possible to ascertain

Save the identity of the person responsible for the authorization to change the SIM card

held on August 5. (…)

It is important in this case to show that the fact of making a

SIM duplication, it does not imply more than access to the telephone line, it would not be

possible access to passwords, bank details and other information of the holder

of the account unless the third party has another series of personal data

of the holder because he had had access to them or had stolen them

previously. Request a loan from the bank or make transactions only for duplication

SIM loss is highly unlikely as we say without having another

type of person information. (…)".

Said claim was resolved by the FILE OF PROCEEDINGS dated

December 2, 2019, in the file with no. of reference E/10004/2019.

SECOND: B.B.B. (hereinafter, the claimant party two), on November 20

2019, files a claim with the AEPD against VDF, for the

following reasons:

"My phone company for poor security measures in terms of

data protection, has allowed to duplicate my SIM card of my phone,

up to three times (November 2, 3 and 12, 2019) to outsiders,

thus accessing all my data and as a consequence of this they have

defrauded my bank accounts by reintegrating all its contents, as well as

apply for loans and open accounts impersonating my identity."

Along with the claim, it provides three complaints with a certificate number

*** ATTESTED.2 dated November 4, 2019; *** ATTESTED.3 dated 5 of

November 2019; and, ***ATESTADO.4 dated November 12, 2019; all

them, presented before the General Directorate of the National Police (hereinafter,

DGPN) in the Madrid-San Blas offices, denouncing these events.

On said claim fell resolution of ADMISSION TO PROCESS dated 2 of

January 2020, in the file with no. of reference E/12065/2019.

THIRD: On November 27, 2019, the director of the AEPD, before the

news appeared in the media regarding the use of practices

fraudulent based on the generation of duplicate SIM cards without the

consent of their legitimate owners in order to access information

confidential for criminal purposes (known as "SIM Swapping"), urges the

Subdirectorate General for Data Inspection (hereinafter, SGID) to be initiated ex officio

the Previous Actions of Investigation tending to analyze these practices and the

existing security measures for its prevention.

Namely:

Vodafone: "They duplicated my SIM and stole XXXX€": the 'SIM swapping' fraud

returns to Spain (elconfidencial.com)

https://www.elconfidencial.com/tecnologia/2019-09-10/sim-swapping-timo-duplicado-

card-scam_2216863/

The Duplicate SIM Scam: If Your Phone Does Weird Things, Check Your Bank Account

| Economy | THE COUNTRY (elpais.com)

https://elpais.com/economia/2019/05/21/actualidad/1558455806_935422.html

The dangerous fashion scam: Duplicate your mobile number to empty your account

bank | Technology (elmundo.es)

https://www.elmundo.es/tecnologia/2020/10/15/5f8700b321efa0c9118b462c.html

FOURTH: C.C.C. on behalf of and on behalf of D.D.D. (hereinafter the part

claimant three), on November 28, 2019, filed a claim with

the AEPD directed against VDF, for the following reasons:

“On September 28, Vodafone gave way a duplicate SIM

fraudulent (SIM swapping) on my husband's card (D.D.D.), entered in

the hospital at the time, suffering from a serious illness.

After many calls to try to stop the fraudulent process, Vodafone

He ignored it and gave the copy of the SIM to the scammer. With this he gave

the access key to our bank accounts and they managed to rob us

money, request loans in my husband's name, payments to bookmakers,

Bizum payments, sale of shares and theft of money, withdrawals of

cash at ATMs...

I want to clarify that we are not claiming any debt or inclusion in

no delinquent file, but the negligence of Vodafone when delivering the

private and financial data of a client to a scammer, giving him the

tool to access bank accounts and steal at will.

Subsequently, and on November 2, my husband passed away, so

it is possible that he makes the claim himself.”

Together with the claim, it provides two complaints with a certificate number

***CERTIFICATE.5, dated October 24, 2019 and ***CERTIFICATE.6, dated October 4,

November 2019. Both presented by their daughter -E.E.E.- before the DGPN

in the dependencies of *** LOCALITY.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

5/88

On October 22, 2019, the claim was transferred to VDF for analysis.

lysis and response within one month.

In response to said request, VDF states -among other arguments- the following:

following:

“(…) the offending person who supplanted the identity of Mr. D.D.D. for the purpose of

manage to change or duplicate the SIM card, (...). To these

effects, the infringer previously knew the personal information of Mr.

D.D.D., specifically, name, surnames, NIF and direct debit account.

Therefore, while all the data was provided correctly to

through (...), for me represented the person who was requesting the

change of SIM was the correct holder, Mr. D.D.D., not being able in any way

notice that said person was not Mr. D.D.D., but a

offender who was impersonating his identity.

In any case, my client wants to emphasize that a change or

duplication of a SIM card implies only the access to the line of

phone associated with it, and in no way offers the possibility that the

operator provides the holder's bank details.

Thus, it is by no means possible to affirm that there is a

responsibility of Vodafone for the actions that occurred in the accounts

bank accounts of ING and Banco Santander of Mr. D.D.D., which will be

reference later.

After carrying out the appropriate investigations, it was found that, on 28

September 2019, after receiving the calls referred to in the

Mrs. C.C.C. in your claim, (...).

(...).

On said claim fell resolution of ADMISSION TO PROCESS dated 25 of

February 2020, in the file with no. of reference E/00557/2020.

FIFTH: F.F.F. (hereinafter, the four complaining party), on November 28

2019, files a claim with the AEPD against VDF, for the

following reasons:

"Last Tuesday, November 12 and 14, I was fraudulently

a SIM copy of two of my three lines that I have contracted with Vodafone,

specifically the numbers ***TELEPHONE.2 and ***TELEPHONE.3. To the

ask in the customer service and in the offices they confirm me

that were made by telephone, without physically requesting the DNI in any

office. No one has explained to me today at Vodafone how it is possible

that anyone who gives my ID number over the phone can receive

a SIM copy of my lines".

On January 22, 2020, the claim was transferred to VDF for analysis.

sis and response within one month.

In response to said request, VDF states -among other arguments- the following:

following:

“

- The "Original SIM" at the time of service registration was assigned

the numbering ***SIM.1.

- On 11/12/2018 a duplicate of the Original SIM is requested by telephone

which becomes the “(…)” numbered ***SIM.2.

- On 11/14/2018 after the activation of the "SIM Bis" its

face-to-face duplicate and becomes "(...)" with ***SIM.3 numbering.

On the other hand, regarding the line of which Mr.

F.F.F., ***TELEPHONE.2, on November 14, 2019, it was verified

that was produced from the store ***TIENDA.1 of Majadahonda a change of

SIM card, going from the initial number ***SIM.4 to the number ***SIM.5, “(…)”.

Similarly, Mr. F.F.F. contacted Vodafone that same day, in order

to report the realization of a duplicate SIM card that he had not

required. Therefore, we are faced with the circumstance that

They requested two changes of SIM cards (...) of the two services of Mr.

F.F.F., one on November 12, 2019, and another on November 14,

2019, which is why the claimant contacted Vodafone upon realizing that

was left without service. Vodafone, in such circumstances, acted

quickly and preventively by blocking both cards

SIM and avoiding possible fraudulent actions that could benefit

of the security gateways used by the means of payment through the

SMS sending.

Vodafone proceeded to restore the service of Mr. F.F.F. on your SIM cards

originals that same day, November 14, 2019, leaving the incidence

resolved. Thus, as of the date of this claim, Mr. F.F.F.

has active and operative SIM cards, having been

Duplicates made fraudulently are automatically cancelled.

(…)

My client wants to highlight the idea that Vodafone is not the cause

of the economic fraud caused to the claimant, insofar as in no

moment has provided or facilitated the information related to the account

to the third party that requested the change of SIM card and that, let's not forget,

managed to overcome Vodafone's security measures because it already had and

knew the personal data of the claimant. In this regard, note that my

represented does not know how the infringer could have access to the data

personal data of the claimant to make use of them. Vodafone just like

that the claimant, has been deceived by a third party, who, knowing the

security mechanisms available to banking entities, knew

that the previous step was to obtain a duplicate of the SIM to be able to receive via

SMS the keys to access the bank information of the claimant,

using it as a preliminary step and a mere instrument to achieve its final objective through

Vodafone. My represented is, therefore, a victim and harmed more in

all this fraudulent artifice, seeing highly compromised and damaged

both its brand image and the trust placed in it by

customers".

On said claim fell resolution of ADMISSION TO PROCESS dated 11

March 2020, in the file with no. of reference E/00558/2020.

SIXTH: G.G.G. (hereinafter, the five complaining party), on December 4,

2019, files a claim with the AEPD against VDF, for the following

reasons:

“As a customer of the telephone company Vodafone with a terminal number

***PHONE.4.

I am writing to this department to inform you that in July 2019 I was

victim of a fraud which was responsible for said telephone company.

Due to the insufficient security policy applied by the company for its

Customers.

Facts

That on August 4, 2019, Mr. H.H.H. contacted me. of

fraudulent transfer department of my bank EVO BANC. The

Mr. H.H.H. informed me that in the early hours of July 29,

made a series of transfers worth €15,000, of which the

security system could only nullify the last ones, amounting to the sum

of 4889 euros.

After having a telephone conversation with Mr. H.H.H., the same

He asked me if I had recently had any kind of incident with the

mobile device. To which I indicated, that effectively on July 29

around 20:00 the terminal had stopped working. Specifically, the SIM of

my number ***TELEPHONE.4, was totally inoperative.

Given the time in which the reported events took place, and given that

Vodafone's physical stores were closed to the public, I

I appeared the next day around 10:30 a.m. in order to find out what

it was happening The store clerk told me that I should make a copy

of the card since the SIM did not work. In order to complete this

process, he asked for my DNI and proceeded to sell and activate the new

SIM card, all this, without verifying the corresponding data, since it does not

I was made to sign any kind of documentation.

As anticipated, Mr. H.H.H. he advised me to call my

telephone company to find out the reason why the SIM card of my

terminal stopped working. After making the corresponding management call

telephone, they confirmed to me that a copy of the

the same on July 29, 2019 from (...).

After locating the data of the aforementioned physical store, I proceeded to contact

contact with the person in charge Mr. I.I.I., who confirmed to me that indeed in the

indicated date, a duplicate of my SIM card was made for the

that the corresponding DNI that appears in the files of the

store.

Given the material impossibility of having carried out this management by my

own person, I asked him to please send me the alleged

presented personal identification document. Lord I.I.I. I indicated

that as a result of the regulations regarding data protection

could not provide me with the documentation.

In view of the foregoing, not having authorized at any time the

issuance of the duplicate SIM card, please send me the

corresponding information about how it could have been authorized such

performance.

In view of the foregoing, and given that a transaction was carried out without the

corresponding authorization and which amounted to the amount of XXXX €, after being

aware of the above situation, I proceeded to file the complaint

corresponding to the police agencies so that the bank can

could refund the amount withdrawn without the corresponding consent

granted by me.

The banking entity, after filing the complaint, informed me that

security would proceed to block all the accounts of which I am the owner.

I have also repeatedly tried to contact the

Vodafone's customer service department, having all turned out

Attempts to resolve this unsuccessful situation.

Together with the claim, it provides the complaint filed for these facts, on the 5th of

August 2019, with procedure number: ***DILIGENCIA.1 before the Mossos

d'Esquadra, OAC of ***LOCATION (Girona); bank certificate issued in that

same date that reports on two transfers made on July 29,

2019 from your checking account in favor of a third party -J.J.J.- for an amount of

2,175.00 euros and 2,713.00 euros.

It also provides a CD-R containing the recording of the telephone conversation

maintained with the Vodafone operator, demanding a security policy that

avoid the reproduction of these facts and a copy of the claim filed with

the Secretary of State for Digital Advancement, with entry record dated 12

September 2019.

On January 22, 2020, the claim was transferred to VDF for analysis.

sis and response within one month.

In response to said request, VDF states -among other arguments- the following:

following:

“After analyzing the claim and investigating what happened, my client has

been able to verify that, on July 29, 2019, it was carried out, from a

physical store of a distributor, specifically, in Santa Cruz de Tenerife, a

change of the SIM card corresponding to the line ***TELÉFONO.4, whose

holder is Mrs. G.G.G.

Specifically, there is a change in the numbering of the original SIM card

“***SIM.6” to the number “***SIM.7” (“(…)”).

Likewise, it was verified that on July 30, 2019, the management

of another change of SIM linked to the same mobile line, carried out, in the

same physical Vodafone store. In particular, there is the change of the SIM

Bis to the numbering “***SIM.8” (“(…)”).

As a consequence, on October 11, 2019, Mrs. G.G.G.

filed a claim with the SETSI, by means of which it revealed the

making a change of the Original SIM requesting to Vodafone: (i) the deregistration

of the services, and (ii) compensation for damages arising from the

fraud, specifically, the amount of XXXX € that it detected had been

transferred from your bank account.

My client responded to said claim, on October 16,

2019, reporting that the change of Original SIM associated with your line of

phone ***PHONE.4 originates from two requests created in a
Vodafone distributor, dated July 29 and 30, 2019. Likewise,
informed the claimant of Vodafone's security policy,
by virtue of which a document must be presented that guarantees the identity
of the applicant to be able to manage duplicate SIM cards.
Regarding the cancellation of the services requested by the claimant, my
represented proceeded to inform him that, while said services were not
had any commitment to stay, manage the discharge
it would mean for her to lose the numbering unless she requested a
portability of its lines to another operator and cause the least damage
possible. (…)
In fact, and after checks carried out on systems, my client
has verified that Mrs. G.G.G. has carried without any charge for
commitment to permanence to the Orange company its mobile lines
***TELEPHONE.5 on February 11, 2020 and ***TELEPHONE.6 on
February 7, 2020.
Subsequently, on November 29, 2019, the claimant
filed a second claim with the SETSI, through which he returned to
point out that, due to the transfers made from your account
bank, requested Vodafone compensation for economic damage
caused. My client responded on December 11, 2019,
indicating that, after verifying the absence of consent in the change of
SIM, thanks to the attached complaint filed by Mrs. G.G.G. before the
General Directorate of the Police and attached to the SETSI claim, the
Vodafone's Quality Department that same day contacted Ms.
G.G.G., in order to explain the existing security processes at Vodafone

that guarantee the security of your client account. It is important to indicate that

was upon receiving this second complaint via SETSI (November 29,

2019) when my client was aware of the possible character

fraudulent processing of SIM changes made in 29 days

and July 30, 2019. (…)

At that time, Vodafone's fraud department studied with

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

10/88

carefully what happened, and cataloged the change of SIM as (...).

In any case, it is in any case proven that the telephone company

is a mere intermediary, who obviously cannot be passed on

responsibility for the management with lack of diligence carried out by

of the banking entity within its security measures".

On said claim fell resolution of ADMISSION TO PROCESS dated 26 of

February 2020, in the file with no. of reference E/00559/2020.

SEVENTH: K.K.K. (hereinafter, the claimant party six), on February 17,

2020, files a claim with the AEPD against VDF, for the following

reasons:

"I am contacting you to denounce the serious situation in the

that I find myself since the Vodafone company provided my data

personal and sensitive to a stranger. Since that day there have been

very serious events and I do not know if other events may occur in the future

Similar.

I enclose several documents to my letter so that you can verify the

events that I will relate below.

On January 5, 2020, at 6:23 p.m., a person pretends to be me

by calling Vodafone customer service and requesting that

send my last phone bill to an email other than me and that

it doesn't even appear in my personal customer data.

The service that I have contracted with said Cía. is that in order to access

I have to do any invoice through my space as a client that I had

Activate with personal passwords and always online. With my client area

I can download my invoices and manage them as I see fit, since that's how

I contracted with them. The invoices contain such important data as my

full name, my ID number, my email address, the

address of my house, all the lines that I have contracted, the extras

contracted as TV and audiovisual platforms (in my case HBO and

NETFLIX) and the last four digits of my bank account. It is not only

irregular that a telephony operator re-send an invoice with said data,

but do it to an email that does not appear in their database. Me

I understand that if someone calls, they must be forwarded to their personal space, and

at most forward an invoice to the e-mail you know to

Vodafone in its database.

From this moment and in 13 calls made by that person

during the afternoon of January 05, 2020, try several SIM changes

(Vodafone says that it can only be done in a physical store), requests from the

PIN and PUK number and purchase intent.

I also have an attempted access to HBO.

Two days later, on January 7, 2020, what Vodafone said happens

that it was impossible. I run out of line around 10:30 in the morning. Is

person makes a call to Vodafone and says they have a SIM to activate,

SIM that we don't even know where it comes from. The operator who attends you

activate the SIM for my phone line and I stop having a connection and no

I can call or receive calls.

I call Vodafone ignoring what happened and ask them to activate the line

Because it does not work. The operator who attends me at no time

notifies me that half an hour before another SIM has been activated, it simply asks me

that facilitates the numbering of my card and by doing so it sends me to the store

physical to make a new duplicate.

Two hours later, at the Vodafone store located in the English Court of

***LOCALITY we processed a change of SIM without them explaining to me what has happened

happened to the line and why it has failed. A few hours later, my wife

(who is a user of one of the lines), receives a text message on her

phone number of your bank (ING Direct), where they inform you that they have

blocked accounts and cards associated with K.K.K. and that you share with him. Us

we miss because I am the beneficiary of their accounts, but I have never

operated or entered the ING Services. We did not give excessive

importance until they definitively blocked all their cards and

accounts (even the ones unrelated to me). ING Direct detects

I try to enter with my identity and my telephone line. Since the moment

in which they had my line with the change of SIM, until

we manage the new one in El Corte Ingles, they have tried to operate in

several banks requesting the resending of passwords to my telephone line

(that person had active).

Fortunately, they did not make attempts at my bank and they did it at

that of my wife, where my ID card appears as beneficiary, but not my phone number because

I have never registered. Luckily, ING Direct Security filters

they have been effective and have prevented a major tragedy for us.

In a Vodafone store located in Barberà del Vallés, a worker

informs us of everything that happened on my lines. I get the list of

operations carried out by that unknown person since the 5th of

January (I enclose this document).

We file a police report at the Mossos d'Esquadra police station

(attached document).

From then on, we have asked Vodafone for explanations on successive

calls requesting measures to ensure that this does not lead to more

consequences and above all that it does not happen again.

They provided me with a telephone service security code that is useless for

nothing because no operator ever asks for it.

I can't override these phone lines because there is a permanence, and

correct is that these numbers cease to be related to me knowing

that someone has so much compromised data.

Vodafone's response as a company (I went to offices in Barcelona

of personal attention) is that nothing has been done wrong and they do not offer me any

exit.

Finally I have had to cancel all the Services (paying almost 300

euros of permanence because of their actions) to make sure that I don't

can follow my trail through Vodafone".

Together with the claim, it provides the complaint filed for these facts, on the 9th of

January 2020, with procedure number ***DILIGENCIA.2 before the Mossos

d'Esquadra USC of *** LOCALITY (Barcelona); and, detail provided by VDF of the

movements made by the person impersonating him.

On March 26, 2020, the claim was transferred to VDF for analysis.

sis and response within one month.

In response to said request, VDF states -among other arguments- the following:

following:

"After analyzing the claim and investigating what happened, Vodafone has been able to

verify that, on January 5, 2020, my client sent a

duplicate of an invoice to the address ***EMAIL.1.

Likewise, on January 7, 2020, my client was also able to

verify that it was made through (...) a change of the SIM card

corresponding to the line ***TELÉFONO.7, associated with the ownership of the

claimant, who was a Vodafone customer on that date.

This part wants to point out that the effective management of sending a duplicate

invoice, as well as the processing of a change of SIM card entails the

overcoming the security policies that Vodafone has implemented

in order to prevent fraudulent practices from being carried out on the data

personal of their clients. In this sense, it has been verified that the

Both procedures were carried out in excess of said policies of

security, so my client understood at all times that

they dealt with legal, real and truthful negotiations.

However, on January 22, 2020, the claimant filed an

claim before the customer service of my client,

claiming that a duplicate of your invoice had been provided to a third party

on Vodafone. It is at this time that Vodafone was aware of

first time of the alleged impersonation of the claimant's identity, when

understand previously that the steps had been carried out lawfully,

truthful and loyal, since the Policies regarding security were surpassed.

From this moment on, my client carried out the investigations and

timely steps, contacting the claimant on 28

January 2020, that is, just six days after having evidence

of the alleged identity theft claimed by Mr. K.K.K., and

also informing him of the security policies that he had

implemented Vodafone.

Additionally, my client wants to point out that it has been verified that

already on January 7, 2020, that is, just two days after

If the duplication of the SIM card took place, my client proceeded to (...).

Said measure also implies that (…). Likewise, and as a result of the activation

of said duplicate as fraud, the line was temporarily deactivated

owned by Mr. K.K.K. My client also warned the claimant

that, in the event that a third party has processed said procedures without your

knowledge, it was possible that such a third party knew in advance the data

personal information relating to your person.

However, and in view of the events that occurred, on February 4,

2020, Mr. K.K.K. voluntarily decided to deactivate all of the

services that it had associated with Vodafone. Thus, on that date

My client processed not only the cancellation of the supposedly affected line

for the processing of the change of SIM (***TELÉFONO.7), but for the rest of the

services associated with the claimant (Fibra ONE 600Mb, Fixed ***TELÉFONO.8,

and mobile lines ***TELEPHONE.9 and ***TELEPHONE.10) and for which no

a duplicate SIM had been managed.

Finally, it is appropriate to point out that changing a SIM card implies

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

bank accounts of the owner, so it does not seem possible to say that there is a

correlation between the actions carried out in relation to the SIM card of the

Mr. K.K.K. and what happened to their bank accounts, in this case, from the

ING entity".

On said claim fell resolution of ADMISSION TO PROCESS dated 16

July 2020, in the file with no. of reference E/03065/2020.

EIGHTH: L.L.L. (hereinafter, the claimant party seven), on March 17,

2020, files a claim with the AEPD against VDF, for the following

reasons:

"They spoofed my identity in a VODAFONE physical store in Girona and

they appropriated the lines contracted by me to VODAFONE. for said

actions performed a SIM card duplication of the mobile line,

leading to economic fraud and consequences

administrative that I continue claiming ".

Together with the claim, it provides the complaint filed for these facts before the DGPN

in the dependencies of ***LOCALIDAD, with certificate number ***ATESTADO.7 in

dated January 4, 2020; and, claim addressed to VDF, dated January 15,

2020, in which it requests that "(…) however, at no time have I expressed

my consent to change the ownership of my services to another person,

We require them to proceed to give explanations about the facts reported in the

this writing, as well as in any case, carry out the necessary procedures and procedures

to make effective the immediate activation of the lines and compensate for the lack of

supply and interruption of service, refraining from charging any amount from

last January 4. 2º.- That this party be informed of how the

produced the change of ownership of my lines, putting at my disposal the

associated voice or documentary recording, in order to carry out legal actions

timely. 3º.- That all the expenses caused by this incident be paid to me,

to cover unfair expenses: purchase prepaid SIM and its top-ups until the

recovery of services, use of telephone booth, reimbursement of the amount

corresponding in the invoices unduly charged to the account, and compensation

for the damages suffered in this VIOLATION IN THE PROTECTION OF

DATA AND IDENTITY THEFT. (…)".

He also provides a bank statement from ING Direct of the current account he shares

with his wife where it is observed that on January 4, 2020 5 charges are made

fraudulent amounts amounting to a total of XXXX.XX euros and two statements of the charges

made through the credit card amounting to XXXX.XX euros.

On June 2, 2020, the claim was transferred to VDF for analysis

and response within one month.

In response to said request, VDF states -among other arguments- the following:

following:

“After analyzing the claim and investigating what happened, my client has

been able to verify that, on January 4, 2020, there were two

ownership changes on the client ID ***ID.1, owned by Mr. L.L.L.

In the first place, there was a change of ownership that associated the data of

a third party, Mr. M.M.M., to the ID ***ID.1 of the claimant. Later, he had

A second change of owner took place that associated the previous client id to the

data from another third party, D. N.N.N.

Likewise, my client has also been able to verify that on the 4th of

January 2020, a SIM change was processed on the line

***PHONE.11, associated with the previous ID ***ID.1. Said SIM change was

managed in person, through a Vodafone store located in

Girona.

This part wants to point out that the effective management of a change of ownership,

as well as the processing of a change of sim card entail the overcoming

of the security policies that Vodafone has implemented, in order to

prevent fraudulent practices from being carried out on the personal data of

Your clients. In this sense, and having processed both procedures

subject to said security policy, my client understood in all

time that they were legal, real and truthful efforts.

However, and in view of the events that occurred, on the same day, January 4

of 2020, Mr. L.L.L. contacted my client, indicating

that the previous steps had been carried out, presumably, without his

authorization, this being the first time that Vodafone had

evidence of the facts that are the subject of the claim. Also, in said

interaction, the claimant requested the blocking of the lines associated with the ID

***ID.1 and informed my client that it was in process

to file a report of the incident with the Police.

In view of the complaint filed with the State Security Forces and Bodies

indicated by the claimant would proceed to file, my client

proceeded to carry out the appropriate investigations and steps in order to

resolve as quickly as possible the incident reported by Mr.

L.L.L. In this way, on January 4, 2020, that is, the same day

in which Vodafone was notified of the events, proceeded to block the

services associated with the ID ***ID.1, restricting in this sense, and as

primary and primary means in the event of a duplicate sim card, the use

of the lines associated with such id. such blockades were carried out with the exclusive

in order to prevent subsequent damage greater than the

claimant.

Likewise, and after carrying out the previously mentioned blocks, the

Vodafone's fraud department proceeded to carry out investigations

opportune, in order to verify if what happened could have the character of

fraudulent and if so, process the change of ownership and SIM to

favor of Mr. L.L.L.

Finally, on January 22, 2020, my client, after verifying

that the previous steps were carried out fraudulently, proceeded to

make a change of ownership of the services associated with the ID ***ID.1,

successfully re-associating them with Mr. L.L.L. Also, on the 23rd

January 2020, my client in turn made a change of SIM on

the line ***PHONE.11 affected, in order to invalidate the SIM card

fraudulently obtained and return control of the line to the claimant.

However, as of January 23, 2020, and because the services

associated with the ID ***ID.1 had previously been blocked by Vodafone,

the client contacted my client, stating that he did not

could make calls successfully. In view of the foregoing, on 26

January 2020, my client proceeded, at the request of Mr. L.L.L., to

eliminate the restrictions on the use of the lines associated with the ID ***ID.1,

re-establishing, therefore, the use of the services already associated with the

claimant. (...).

Finally, it is also appropriate to point out that the exchange of a card

SIM only implies access to the telephone line associated with it, not

to the holder's bank details, so it does not seem possible to say that

there is a correlation between the actions carried out in relation to the

SIM card of Mr. L.L.L. and what happened to their bank accounts, in this

case, belonging to the entity ING".

On said claim fell resolution of ADMISSION TO PROCESS dated 24 of

July 2020, in the file with no. of reference E/03632/2020.

NINTH: Ñ.Ñ.Ñ. (hereinafter, the eighth claimant), on June 30, 2020,

files a claim with the AEPD against VDF, for the following

reasons:

Ñ.Ñ.Ñ., with DNI

***NIF.1, resides in Seville. w/

“The exponent,

***ADDRESS.2. On June 2, 2020, around 1:00 p.m., he noticed

that it did not have a telephone line, something that it could not solve until the day

next June 3 around the same time you buy a new card.

From the investigations and accompanying documents it can be deduced:

1.- Some strangers, without being duly accredited, because they were not

requires the DNI, they buy a telephone card in Valencia in my name, and

they celebrate a new contract with Vodafone, also in my name. in said

Vodafone contract provides you with my bank account to be charged at the Bank

Santander.

2.- With such data, request my electronic signature by phone from the bank, my

credit card data and rob the account owned by the interested party

in said bank.

Together with your claim, you submit a request addressed to VDF dated June 8, 2020

in which he demands that "said events not occur again, keep the tapes

of video surveillance of the Carrefour Valencia store and, where appropriate, put them to

disposition of the police to investigate the facts and to compensate the interested party in the

amount in which it has been harmed; 17,265.00 euros missing from

the current account (…)".

It also accompanies another claim addressed to VDF via email, dated June 10,

2020, in which he reiterates his requests.

It also provides the invoice issued by VDF, dated June 2, 2020, with the

number ***FACTURA.2, which contains the charge corresponding to the issuance of a

SIM card, where you specify as delivery address a company called

(...) located in the municipality of *** LOCALITY (Valencia), when the CLAIMANT

OCHO has its habitual residence in the municipality of SEVILLA.

It also accompanies the Mobile, Broadband, Landline and TV Service Contract for

Private Clients who deny having subscribed in the municipality of ***TOWN of

date June 2, 2020 and the claim of operations carried out through the

Visa/MasterCard credit card in your name, addressed to Banco Santander by the

more than 20 transactions carried out between June 2 and 4, 2020, which

exceed XXXX.XX euros.

It also adds the complaint filed on June 12, 2020 before a branch

of VDF located in Malaga for the events that occurred.

On July 17, 2020, the claim was transferred to VDF for analysis

and response within one month.

In response to said request, VDF states -among other arguments- the following:

following:

"After analyzing the claim and investigating what happened, Vodafone has been able to

verify that, on June 2, 2020, a SIM change was processed

on the line ***TELEPHONE.12, associated with the customer ID ***TELEPHONE.13,

which the claimant owns. Said change of SIM was managed in

in person, through the Vodafone Point of Sale operated by (...),

located in *** LOCATION, Valencia.

This part wants to point out that the effective processing of a card change

SIM entails overcoming the security policies that Vodafone has

implemented in order to prevent fraudulent practices from being carried out on

the personal data of its customers. In this sense, and having processed

said change of SIM, treating said management of an operation subject to the

overcoming the security policy of Vodafone, my client

understood at all times that it was a management with the appearance

lawful, real and truthful.

Notwithstanding the foregoing, on June 3, 2020, the claimant

contacted my client, indicating that he did not have

coverage on your device associated with the mobile line ***TELÉFONO.12,

this being the first time that Vodafone was aware of the

incident object of claim. In this way, my client made

timely investigations and procedures, being able to confirm that the reason

for which the claimant did not have coverage was due to the SIM change

processed the day before. In view of the foregoing, my client proceeded to

process a new SIM change, in order to cancel the change made in

date June 2, reestablishing for this purpose the line and control over the line

***TELEPHONE.12 to Mr. Ñ.Ñ.Ñ. on June 3, 2020, that is, a day

after becoming aware of the incident that is the subject of the claim and in

In any case, prior to receipt of this request by

part of the Agency.

Likewise, my client was also able to verify that, on the date of

June 2, 2020, a modification order on services was processed

associated with the previous customer ID, in order to modify the Vodafone services

One Fibra 50Mb + M + TV + Total + Fixed enjoyed by Mr. Ñ.Ñ.Ñ. by

Vodafone One Unlimited Total Fiber 1Gb rate. Furthermore, this order

in turn intended to deactivate the claimant's Vodafone TV services.

Said modification order was also managed in person, through

through the Vodafone Point of Sale operated by (...) located at

***LOCATION.

As for the processing of a SIM change, the modification of the

services and rates activated to the ID of one of Vodafone's customers entails

overcoming the security policies that Vodafone, in order to prevent

that fraudulent contracts are made on the personal data of

its clients that could cause economic damage to them by

the contracting of unrecognized services. In this sense, and having

embodied the service modification order under a contract, which is

provides as Document number 2, my client understood in all

moment that was before a management with the legal, real and truthful appearance.

Notwithstanding the foregoing, due to the interaction between the claimant and

my client dated June 3, 2020, and because the order of

Modification of services was also processed from the same Point of Sale

on which the fraudulent SIM change had been processed, my

represented proceeded to interrupt the process of activating the tariffs

contracted, in order to avoid causing any damage to Mr. Ñ.Ñ.Ñ. (…)

Lastly, my client considers it opportune to indicate that the change of

a SIM card implies only access to the associated telephone line

to it, not to the holder's bank details, so it does not seem possible

affirm that there is a correlation between the actions carried out in relation to

with the SIM card of Mr. Ñ.Ñ.Ñ. and what happened to their bank accounts."

On said claim fell resolution of ADMISSION TO PROCESS dated 28 of

August 2020, in the file with no. of reference E/05844/2020.

TENTH: O.O.O. (hereinafter, the claimant party nine), on June 8, 2020,

files a claim with the AEPD against VDF, for the following

reasons:

"On January 7, 2020, my terminal lost its line, being in the

office I do not give it more importance since I am still connected to the wifi, to

Then I get a message from ING Direct to confirm a

operation that I have not performed, I see this message when I go down to

breakfast, so since I don't have a line I can't deny the operation. A

Through another mobile I can contact Vodafone because I suspect that

They have duplicated my SIM and they are doing fraudulent operations in

Bank entities.

When I call Vodafone they tell me that I am not the owner of the line, that

has just produced a change of owner (without my consent). I indicate

that it is a fraud, they mark it (or so they say) as such and agree to call me

urgently. This call never occurs, so about 8 hours

then I call again and it turns out that they have changed the ownership of

the account to a different person...

In short, without my consent they make a change of owner, they let me

without a line for 2 weeks and they make a duplicate SIM that they take advantage of to access

to ING Direct accounts, request a loan in my name and withdraw cash 5

a thousand euros..."

Along with his claim, he provided the complaint filed for these facts, on the 7th of

January 2020, with certificate number ***ATESTADO.8 before the DGPN in the

dependencies of ***LOCALITY.

Likewise, it provides the invoice number ***FACTURA.3 issued by VDF in the same

date, which contains the charge corresponding to the issuance of a SIM card, where

specifies as delivery address ***ADDRESS.3 in the municipality of

*** LOCATION (GIRONA), when CLAIMANT NINE has his residence

usual in the municipality of *** LOCATION (LAS PALMAS).

It also provides the claim addressed to VDF on January 8, 2020 requesting

an explanation of the two changes of ownership produced in your line and the issue

of a SIM card, without your consent and the following messages exchanged

with the VDF Customer Service, in response to your claim.

On June 23, 2020, the claim was transferred to VDF for analysis

and response within one month.

In response to said request, VDF states -among other arguments- the following:

following:

“After analyzing the claim and investigating what happened, Vodafone has been able to

check that, (…).

Likewise, my client has also been able to verify that on the 7th of

January 2020, a SIM change was processed on the line ***TELÉFONO.13,

associated with the ID ***ID.2 above. Said SIM change was (...).

This part wants to point out that the effective management of a change of ownership,

as well as the processing of a change of SIM card entail the overcoming

of the security policies that Vodafone has implemented, in order to

prevent fraudulent practices from being carried out on the personal data of

Your clients. In this sense, and having processed both procedures

subject to said security policy, my client understood in all

time that they were legal, real and truthful efforts.

However, in view of the events that occurred, on the same day, January 7

2020, the claimant contacted my client, indicating

that the previous steps had allegedly been carried out without his

authorization, this being the first time that Vodafone had

knowledge of the facts object of the claim. In this sense, my

represented proceeded to carry out the appropriate investigations and procedures,

in order to resolve the incident that occurred and make the change of ownership and the

change of SIM that returned control of both the line and the ID

concerned, Mr. O.O.O. Therefore, on January 9, 2020, that is, as

only two days after having proof of the facts object of

claim, and after verifying that he was dealing with procedures that, despite having the
appearance of truth, were of a fraudulent nature, my client
proceeded to block the client's account, restricting the use of services
associated with ID ***ID.2. Such blockade was carried out with the sole purpose of avoiding
that greater damage could be caused to the claimant O.O.O. Y
deactivating the previous third parties that were unduly listed as
claimant account holder. (…)
Likewise, on January 13, 2020, the claimant made, in turn,
in person at a Vodafone store, a change of SIM on the line
***PHONE.13 affected, which allowed invalidating the previous SIM card
fraudulently duplicated, thereby returning control of the
line to the claimant. (…)
Therefore, my represented managed to solve the incident object of
claim effectively on January 13, 2020, when he processed the
change of SIM on the affected mobile line that, together with the change of
ownership made on January 9, 2020 on the ID ***ID.2, they returned the
full control of the lines to Mr O.O.O. In this sense, the incidence was
correctly resolved in internal systems of my represented with notorious
prior to receipt of this request by the
Agency.
Finally, it is appropriate to point out that changing a SIM card implies
only access to the telephone line associated with it, not to the data
bank accounts of the owner, so it does not seem possible to say that there is a
correlation between the actions carried out in relation to the SIM card of the
Mr. O.O.O. and what happened to their bank accounts."
On said claim fell resolution of ADMISSION TO PROCESS dated 2 of

September 2020, in the file with no. of reference E/05287/2020.

ELEVENTH: In view of the facts denounced in the different claims,

the documents provided by the claiming parties and the agreed Internal Note

by the director of the Agency, the SGID proceeds to carry out preliminary actions

of investigation for the clarification of the facts in question, by virtue of the

investigation rights granted to the control authorities in article 57.1 of the

Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter

RGPD), and in accordance with the provisions of Title VII, Chapter I, Section se-

second, of the LOPDGDD.

Within the framework of the previous investigation actions, three requirements were made:

Information requests addressed to VDF, on different dates:

Secure Verification Code Requirement

First

Second

Third

***CSV.1

***CSV.2

***CSV.3

Required date

I lie

Notification date-

tion required

I lie

01/13/2020

01/16/2020

06/12/2020

01/15/2020

09/15/2020

09/16/2020

In the first of the requirements, dated January 13, 2020, the

Next information:

1. Information on the channels available to customers to request a duplicate

SIM card crash. (Telephone, Internet, shops, etc.).

2. For each of the routes available, detailed information is requested

of the procedure established for the attention of the requests, including the

controls for the verification of the identity of the applicant including the data and

documents required from the applicant, as well as the details of the verifications

tions that are made on them. In case of shipment of SIM card by co-

mail, detail of the controls and requirements established on the direction of delivery

he saw.

3. Instructions given in this regard to the staff that attends the requests for

their attention. Documentation proving its dissemination among the companies

employees dedicated to said tasks, internal or external to the entity.

4. Information on whether the performance of the controls to verify the

identity is reflected, for each request attended, in the Information System

mation of the entity. Documentation that accredits it in your case, such as

screen pressure of the buttons (check-box) or other documentation according to the

method used.

5. Reasons why it has been possible in some cases to supplant the

identity of clients for the issuance of SIM duplicates. Reasons why

The implemented security measures and controls have not had an effect.

6. Actions taken by the entity when one of these cases is detected.

Information on the existence of a written procedure and a copy of it in

affirmative case. Actions taken to prevent cases of this type from occurring

produce again, specifically, changes that may have been made on the

procedure to improve security.

7. Number of cases of fraudulent duplicate SIM requests detected

two throughout the year 2019.

Total number of mobile telephony clients of the entity.

In the second of the requirements, dated June 12, 2020, the

Next information:

POINT 1. Clarification is requested on the following aspects in relation to the

response to our request dated January 16, 2020, on the mar-

co of this same file:

A). At the end of the FIRST statement of the answer it is mentioned that

processing is only possible (...) in three cases ((...)). Nevertheless,

in point 2 of the THIRD manifestation it is mentioned that (...).

A copy of the written procedure is requested where all the cases that

are processed (...), including all assumptions.

A copy of the specific instructions given to operators with information is requested.

detailed information of how the operator values all the assumptions, including

how do you assess or check (...).

B). In relation to the data for the identification of the client that is requested during

you a duplicate request (...). In the SECOND manifestation it is mentioned

which is requested "(...)", in addition (...). However, in point 2.a) of the statement

THIRD tion is said to ask for "(...)".

A copy of the security procedure/policy is requested where it is clearly stated

the data that is requested according to the different cases, including all the sub-

posts.

A copy of the specific instructions given to operators with information is requested.

detailed information of the data that must be requested in each case.

C) About the application process (...). Copy of the process followed by clients,

including the steps they must take and the data they necessarily provide.

D). Checks that are carried out in the home delivery of the SIM card

for recipient identification. Copy of the contractual documentation with

the logistics/courier companies that carry out the distribution, where the

identity checks to be carried out by the delivery person.

E) Copy of the periodic communications sent to the points of sale, channel

phone and the logistics operator about the risks and policies in this regard,

mentioned in the FOURTH statement of his answering brief.

POINT 2. List of 20 cases of SIM duplicates reported/claimed as

identity theft or fraudulent by customers. The list will include duplicates

SIM claims requested since January 1, 2020, that is, all claims

two that happened from January 1, from the first, consecutive until reaching

gar to 20 (these are cases that have not been the subject of a claim before the AEPD).

It is requested to indicate in the list the date, the line number and the channel of the request.

POINT 3. About cases presented before this Agency that are summarized in the table

(which is fully reproduced in this act of procedure):

Reason why in case E/10004/2019 when the client calls indi-

It is requested:

A.

When you do not have a line, you are not alerted that your SIM has been duplicated.

b.

Reason why in cases E/12065/2019 and E/00558/2020 no

taken into account the recent shipments of SIM duplicates and has achieved

duplicate the SIM repeatedly.

Written procedure or instructions that exist on how to consider possible

future identity theft cases in a given client with precedence

teeth.

In the cases of request in store, copies of the DNI collected in the so-

c.

SIM duplication request. If there is no collected copy, reflection that is recorded in

the systems of the application and verification of the identity of the applicant

upon display of your ID.

d

For the cases of application (...), information on whether there is a requirement

site for delivery that the city where the SIM is requested is the city of residence

customer dence. Information on whether there is any additional control in case of

different cities.

AND.

the call, and printing of the case registered in the entity's systems).

F.

In cases of request (...), with delivery of SIM to home, justification

of the reasons why the SIM could be delivered to an address other than the one

of the client if said channels are not allowed with a previous change of address. In-

training on whether duplicate addresses were set in requests

new delivery.

g.

documentation of the following aspects:

Actions undertaken by VODAFONE in each case, including accreditation

In the cases of request (...), record of the case (Providing recording of

~

If you have been marked as a victim of customer fraud to avoid possible

future phishing attempts.

- If internal investigations have been carried out to clarify the facts

either with the point of sale in case of store delivery, or internal

in the case of an online/telephone channel.

~

If the client has been contacted to alert him of what happened and about

the resolution of your case.

In the third and last of the requirements, dated September 15, 2020,

requested the following information:

POINT

1. Regarding the list of 20 cases of SIM duplicates reported/claims

detailed data provided in the previous answer (given in full)

reproduced in this act of procedure):

It is requested, in cases of face-to-face application, a copy of the DNIs or documents

two.

On the cases presented before this Agency that are summarized in the

identification provided by the applicants in the change of SIM.

In the case of telephone requests, a copy of the recording of the conversation

where the applicant exceeds the security policy.

POINT

table:

It is requested:

A) Case E/3065/2020: Regarding the call answered on 5/1/2020 from a

person requesting a copy of an invoice. A copy of the recording of the call is requested.

mada where the security policy is exceeded by the caller.

Copy of the submitted invoice.

Copy of the call log with the operator's comments, as well as the

reason why it is sent to an email address that does not appear

in customer data.

Copy of the record of the multiple SIM change attempts made on

5/1/2020, PIN and PUK requests and purchase attempts.

Copy of the SIM change/activation record made on 7/1/2020. Recording

of the call where there is a record of the verifications of the identity of the

applicant (exceeding the privacy policy).

Reason for SIM change after multiple attempts

suspected of fraud. Reason why the customer is not marked as fraud

until 7/1/2020, and SIM change is allowed.

Reason why the customer is not alerted of the previous SIM change, when calling

on 7/1/2020 when noticing that he does not have a line, indicating him by VODAFONE

to request a change of SIM in person.

Copy of customer call log, dated 7/1/2020 where customer

announces that he has lost his line.

B) Case E/3632/2020: In relation to changes of ownership prior to the change

of SIM, a copy of the recording of the calls is requested where the policy of

security by the caller.

Copy of the record of the call and the steps taken with the comments

of the operator for the changes of ownership of 4/1/2020.

For the face-to-face SIM change on 4/1/2020, a copy of the DNI or documentation is requested.

Identification document collected in the SIM duplication request.

C) Case E/5844/2020: For the new contract or change of contract of tele-

phone of 6/2/2020, a copy of the DNI or identification document collected in

face-to-face hiring.

Copy of the new contract delivered to the contracting party.

For the face-to-face SIM change on 6/2/2020, a copy of the DNI or documentation is requested.

Identification document collected in the SIM duplication request.

D) Case E/5287/2020: In relation to changes of ownership prior to the change

SIM bio, a copy of the recording of calls is requested where the capacity is exceeded.

security policy by the caller.

3.

Copy of the record of the calls and the steps taken with the comments

of the operator for the changes of ownership of 7/1/2020.

Copy of the records of the calls made by the client alerting that

does not have line operator comments for ownership changes

from 7/1/2020.

There are two changes of ownership, calling the client between the two

alerting of not having a line and possible change of SIM. justification that

can contribute so that the second change of owner takes place after the

customer alert.

Reason why an alert has not been included so that no more occur

allegedly fraudulent changes.

For the face-to-face SIM change on 7/1/2020, a copy of the DNI or documentation is requested.

Identification document collected in the SIM duplication request.

On the cases in which a SIM is delivered in person in

POINT

store and it is activated by telephone, or there is a theft of SIMs in the store (see chapter

are E/12065/2019, E/00557/2020, E/00558/2020).

It is requested:

~

Information on whether it is possible to acquire SIMs sent to the store by Vodafo-

ne without associating them to any line or client. Causes for which it is allowed

that a customer takes a SIM from a store without activating and without being associated with a

determined line, and it is later allowed to activate the telephone

SIM and associate to a line.

Information about the cases, which do not involve a possible SIM fraud

swapping, in which a client can be in possession of a SIM without

have been previously associated in the entity's systems to a line

of its ownership.

Security policy that is passed to the applicant in the collection of the SIM when

do not associate to a line or customer during its collection.

Causes for which it is allowed in the procedure to activate by telephone

any SIM for a given line. (Case of stolen SIMs in

a store, which are found unassociated with any customer or line).

~

~

~

Regarding changes of ownership by telephone, a Security Policy is requested that

is passed to the applicant. Copy of the specific instructions that in this regard dis-

put the operators.

TWELFTH: On June 23, 2020, VDF requests an extension of the deadline

Given the impossibility of collecting and structuring the information required within the established period,

established.

On June 29, 2020, the Deputy Director General for Data Inspection

agrees to extend the deadline for a period of five days.

TENTH

the next information:

THIRD

: In response to the three requirements formulated, VDF provides

Regarding the first of the requirements, the information is specified in accordance with the

Required sections according to numbering order:

1.- Information on the routes available to customers:

(...).

2.- Detailed information on the procedure:

(...).

3.- Instructions issued to the staff:

(...).

4.- Information on the registration of information in the system:

(...).

5.- Reasons for which the identity theft of clients has been possible:

(...).

6.- Information on the existence of a written procedure:

(...).

In relation to the existing procedure or instructions on how to

Evaluate possible cases of future identity theft in a given

client with precedents, (...). Likewise, (…). They have provided a copy of the

notices sent in the last year.

7.- Number of cases of fraudulent requests for duplicate SIMs detected during

throughout the year 2019.

(...).

Regarding the second of the requirements, the information is specified in accordance with the

points required according to the order of numbering:

POINT

1:

A). Copy of the procedure and instructions:

(...).

B). Copy of the procedure or security policy:

(...).

C). About the online application process:

(...).

D). Copy of the contractual documentation with the logistics/courier companies

jería that carry out the distribution:

(...).

AND). Copy of the periodic communications sent:

(...).

List of 20 cases of SIM duplicates reported/claimed as

two:

POINT

identity theft or fraudulent by customers:

(...).

POINT 3: About cases presented before this Agency:

 File E/10004/2019:

It states that after analyzing the reason why the client was not alerted of the du-

SIM card at the time the call was made, they have verified

do that the fraudulent duplicate was made on 08/05/2019 at 8:38 p.m.,

but until 11:08 p.m. the claimant does not call customer service. (...).

However, the claimant has stated about the call (does not indicate time,

but after 9:00 p.m.) that “after 2 minutes of waiting they tell me that the line

is fine and go to a dealer (Vodafone store) to see if it works.

It may be a problem with the SIM card, which may be damaged and

that is solved with a change of it”. It also indicates that on the following day

next, since he works in a town where there is no Vodafone store,

could not go to a store until 6:30 p.m. and at 7:04 p.m. when he retrieved the

line receives alert from your bank wire transfer. On 08/07/2019 I discovered

open in a branch of your bank more than 25 expense operations

fraudulent.

The duplicate has been made in a Vodafone store in a city other than that of

claimant's residence on 08/05/2019 at 8:39 p.m.

VDF indicates that (...).

VDF has not contributed (...).

□

File E/12065/2019:

□ The first SIM change is made on 11/1/2019 at 23:23:22 for each

telephone end. The SIM change request is made from a call to the

customer service from hidden number.

□ The second dated 11/4/2019 6:30:23 on the My Vodafone Web channel using

do the SIM card ***SIM.9.

□ The third dated 11/12/2019 11:58:03 on the Mi Vodafone Web channel, using

do the SIM card 5***SIM.10.

□ (…).

□

File E/00557/2020:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Indicates that a SIM change can only be carried out

by overcoming the security policies you have in place

to prevent fraudulent practices from being carried out on the data of its clients.

you. It states that the offending person who impersonated the client's identity in order to

of being able to change or duplicate the SIM card, it was required (...).

Indicates that the infringer previously knew the customer's personal information, in

concrete, (…). Therefore, while all the data was provided in a co-

right through Customer Service, for Vodafone the person who

was requesting the change of SIM was the correct owner, not being able to

warn that said person was an offender who was impersonating his

identity.

It also indicates that, after conducting the appropriate investigations, it was found that,

on September 28, 2019, after receiving the calls to which he refers

in the claim, the Vodafone fraud department studied

He carefully gave what happened, and this case (...).

It also indicates about this case that on 09/28/2019 21:03:16 from the department

In case of fraud, the change of SIM is detected and temporary deactivation is applied to the

line so that it cannot be used to make calls or transactions.

The client is contacted on 09/28/2019 where it is confirmed that said client

has not made any changes, but indicates that it can no longer attend to the

call.

(...).

Prior to the change of SIM carried out by telephone, it is sent to the distributor.

(...).

□

File E/00558/2020:

It has indicated that according to the information contained in its systems, it can be

prove that the SIM duplicate attempts were canceled and not processed at

complete from the moment in which the commission of the fraud was confirmed.

of. They provide a screen print indicating that "on 11/12/2019 the

A fraudulent duplicate SIM card was carried out and on 11/14/2019 there was a

attempt from the On-line channel, but the orders appear cancelled" (they refer

to the orders of the day 11/14/2019, which are two). Vodafone has indicated for another

case that “when an order is completed the status appears as closed”. In the

screenshot provided, the order of 11/12/2019 appears as closed, and the orders

dated 11/14/2019 appear cancelled.

The SIM change on 11/12/2019 was made (...) and on 11/14/2019 via (...).

It reports that “given that the first SIM change is made by (…) it is transferred

dated 11/19/2019 information to the person in charge of customer service so that

reinforce the security policy and review actions with the agent/agency.”

Likewise, it indicates that on 12/05/2019 at the request of the fraud department

“the option of (…) was closed”.

Reports that after analyzing the origin of the SIM cards, both come from the

same batch of 100 cards sent to a dealer. Information was requested and

documentation to the distributor in question so that he could credit who had been

delivered the SIM card. The dealer confirms that he does not have the documentation

tion.

File E/00559/2020:

VDF has not provided a copy of the applicant's DNI, alleging that it was requested from the

store the document provided for the collection of the SIM card and that they had

of said document, which was manipulated. They indicate that the distributor was not penalized

buyer since it complies with the guidelines set by Vodafone in these cases.

you are

Regarding the third of the requirements, the information is specified in accordance with the

points required according to the order of numbering:

POINT 1: (these are cases that have not been the subject of a claim before the AEPD).

 Copy of the DNIs, with respect to which the following is verified:

(...).

 In telephone requests, a copy of the recordings of the conversation:

(...).

POINT 2:

File E/03065/2020 regarding which it states the following:

They indicate that the recording of the call is not carried out in all interactions.

tions that are made with calling customers or people interested in the

Vodafone products, since it is not strictly necessary for the good

development of the provision of customer service, such as the

case. Indicate that (…).

(...).

They indicate that these interactions were not only identified by the caller

as a SIM change, but were masked within other SIM requests.

support, making it difficult to determine such actions as fraudulent,

especially when the customer service was provided by different

operators.

They indicate that it is not possible to collect the recordings of the calls made

for the change of SIM cards given that the period of conservation of this

has expired. The interaction made by the caller in which it is shown is recorded.

Against the operator's assessment of overcoming the security policy “pol.

Ok client requests change of SIM that you have received”.

They have indicated that the different attempts to obtain the change of SIM are identified

fy before the customer service under different incidents, resulting in

the identification of these more complex fraudulent behaviors, especially when

when the caller exceeds the security policy.

(...).

They state that at the moment in which the client realizes that he does not have a line,

its client has no evidence that it has previously occurred

fraudulent behavior since, when the SIM is changed, it is added

per security policy.

(...). As this incident persists, the client is instructed to duplicate the

SIM. It is after these interactions, on January 7, 2020, when the

Vodafone's fraud department identifies that the customer is the victim of a

fraudulent conduct, moment in which they state that the whole process begins

relevant to remedy this situation.

They also indicate (on January 9, 2020) that the client himself contacts

tact with customer service stating that you want to request a double password

because they were trying to impersonate his identity. In that

At this time, VDF informs the client that there is no possibility of a double classification.

sees, so it is determined with the client to modify the one he has. manifest

that this interaction shows that VDF acted with the utmost diligence.

Regarding the copy of the customer's call record, it is verified that it consists

in the interaction with the client as a solution to the incident "you are instructed to do

duplicate card.

File E/03632/2020:

VDF does not provide these recordings stating that it is not possible to provide the

recording of the call given the storage limitations of the systems

as there are millions of calls to customer service that generate

would require a high volume of recordings to be safeguarded, and that overcoming

The security policy is an intrinsic procedure to the customer service.

client that all operators go through before providing any information.

mation.

They provide printing of the screens, consisting of operator notes only-

“(…)” for the first change (the same change is made twice consecutively).

day, canceling the first) and "I confirm the change of owner of ***TELE-

PHONE.11” for the second change.

There is interaction by call from the client on the same day in which the claimant-

He tells you that he has not requested a change of owner or change of SIM.

VDF has provided a copy of the DNI provided by the applicant (the new owner). The

copy of the DNI provided is incomplete, the DNI being chopped up and missing.

taking a small piece of it.

File E/05844/2020:

VDF states that it is not possible to provide said document as the points of
sale those who carry out the verification and copy of the DNI to carry out the
face-to-face hiring. It is the points of sale themselves who guard the
copies of the DNI and make them available to VDF. In the present case,
can that they have verified that it was managed in a store of (...).
They provide a copy of an unsigned PDF contract containing the
data of the claimant and his ID number, dated 06/02/2020, giving
drop certain services. The data of the new client and an account
bank that coincides with that of the claimant. The document is
digitally written by the new customer, but not by the old one, the claiming party
you eight
They indicate that it is not possible to provide a copy of the DNI as the points of sale pre-
essential those who carry out the verification and copy of the DNIs to carry out
SIM duplication. It is the points of sale themselves who guard the
copies of the DNIs and make them available to VDF. In the present case,
can that (...).
They do provide screen prints that reflect the management in relation to the
SIM application. They indicate that the screen prints show the different
interactions carried out in which the digital signature of the applicant and the
SIM change order. It is observed that the name appears on the screens
of the new owner.

File E/05287/2020:

VDF does not provide these recordings stating that it is not possible to provide the
recording of the call given the storage limitations of the systems

as there are millions of calls to customer service that generate

would require a high volume of recordings to be safeguarded, and that overcoming

The security policy is an intrinsic procedure to the customer service.

client that all operators go through before providing any information.

mation.

VODAFONE representatives provide screenshots reflecting

jan interactions that are listed in successive order in time (see number in-

teraction):

~

~

~

~

~

~

C/ Jorge Juan, 6

28001 – Madrid

Interaction ***INTERACTION.1: the owner is changed.

Interaction ***INTERACTION.2: the owner change produced is reported.

Interaction ***INTERACTION.3: the headline asks about the change produced

do and want to cancel it.

Interaction ***INTERACTION.4: the client is helped to attend to his request.

Interaction ***INTERACTION.5: the client calls informing about the pre-

total identity theft.

Interaction ***INTERACTION.6: new request to change the owner, modi-

fication only the owner.

Interaction ***INTERACTION.7: the change of owner is confirmed:

Interaction ***INTERACTION.8: Fraud request is opened

~

~

It alleges that after the first change of ownership, the client gets in touch

contact customer service to report that you are having problems with

your line and, later, it is identified that it may be a fraud action. In-

say that during the time that VDF carried out the pertinent actions

To determine the existence of an assumption of fraud, various

interactions between Vodafone and the different parties involved, all of them with the appearance

truthful experience that they are presumed to pass the security policy.

In no interaction is it reflected that it has passed or has not passed the

security policy.

They state that, on the same day, January 7, 2020, VDF carried out

the pertinent actions to protect the interests of the client, blocking the

lines until the Vodafone fraud department determined the actions

tions to develop. It is not reflected on the screens.

(...).

Provide a copy of the DNI provided by the applicant (of the new owner). The copy of

DNI provided is incomplete, the DNI being cut into pieces and one piece missing.

zo of this It is also noted that it is the same DNI as for the claimant.

keep seven.

POINT 3

Information on whether it is possible to acquire SIMs (…);

(...).

Information on the cases (…):

(...).

Security policy that is passed to the applicant when collecting the SIM (...);

(...).

Causes for which it is allowed in the procedure to activate by telephone

a SIM (...):

(...).

About changes of ownership by telephone (...):

(...).

FOURTEENTH: On August 27, 2020, information is obtained from the

National Commission of Markets and Competition on telephone lines

mobile voice by type of contract and by segment, the results being:

OPERATOR

PREPAID

VODAFONE

Residential

2,066,349

Business

0

POSTPAID

Residential

6,867,903

Business

3,487,812

FIFTEENTH: On January 25, 2021, commercial information is obtained

on the volume of sales of VDF during the year 2019 being the results of

3,635,853,000 euros. The share capital amounts to 439,110,908.20 euros.

SIXTEENTH: On February 8, 2021, the director of the AEPD agrees

initiate a sanctioning procedure against VDF, in accordance with the provisions of the articles

Articles 63 and 64 of Law 39/2015, of October 1, on Administrative Procedure

Common Public Administrations (hereinafter, LPACAP), for alleged

Violation of article 5.1.f) and 5.2 of the RGPD, typified in article 83.5.a) of the RGPD

and in article 72.1.a) of the LOPDGDD.

The Start Agreement is notified to VDF, on February 10, 2021, through the

Electronic Notification Service and Authorized Electronic Address, according to

certificate in the file.

SEVENTEENTH: On February 11, 2021, VDF submits a letter to

through which it requests the extension of the term to submit allegations and provide documents

ments or other elements of judgment, and in addition, the remission of the sanctioning file.

EIGHTEENTH: On February 17, 2021, the examining body agrees to the

requested extension of the term up to a maximum of five days, as well as the remission of the

copy of the file, in accordance with the provisions of articles 32.1 and 53.1 a) of the

LPACAP.

The Extension Agreement is notified on February 22, 2021.

NINETEENTH: On March 3, 2021, this Agency received, in

time and form, written by the lawyer and representative of VDF, which proceeds to

formulate allegations and in which, after expressing what was appropriate to his right,

ends by requesting the dismissal of the file with the consequent filing of the

actions since none of the imputed infractions have been committed and

subsidiarily, in case of imposing a sanction, the imposition of an amount

minimum, in light of the mitigating circumstances alleged.

In summary, it states that:

1.- VDF had not infringed articles 5.1.f) and 5.2 of the RGPD, since it had

Appropriate technical and organizational measures have been applied to ensure

level of security appropriate to the risk.

2.- There was no fault in the imputed infractions and consequently, could not

impose any penalty.

3.- In the event that it was understood that it was appropriate to impose a sanction,

extenuating circumstances should be taken into account.

4.- It enumerated the evidence that they intended to use.

VDF alleged the following arguments:

First.- The adoption of technical and organizational measures is not an absolute obligation.

solute. VDF has complied with the principle of integrity and confidentiality and with the

obligation to adopt appropriate technical and organizational measures.

I.- Invokes the Judgments of the National High Court (hereinafter, SAN) (Chamber

of the Contentious Administrative, hereinafter, SCA) of February 25, 2010

[JUR 2010/82723] and November 10, 2017 [JUR 2018/3170]) (…). So

Therefore, the fact that a third party has overcome these measures does not imply,

per se, having breached the obligation or, as the case may be, the principle of integrity and

confidentiality. The data controller is subject to an obligation to

means, not to an obligation of result in the sense of understanding that all in-

accident is a breach of the duty to "guarantee a level of security

appropriate to the risk" (article 32 of the RGPD).

II.- VDF is responsible for adopting technical and organizational measures aimed at

that duplicate SIM cards be provided to holders of lines

telephone. In this sense, the following behaviors fall outside the sphere

VDF control:

1.- The behaviors carried out by the scammer or cybercriminal in a

Stage prior to requesting the duplicate SIM card:

(...).

2.- The behaviors carried out by the scammer or cybercriminal in a

stage after the request for the duplicate SIM card, such as

example access to online banking applications of victims and

carrying out fraudulent operations through said applications.

nes.

Refers to folios 291 and following of the file where BBVA puts

It is clear that it is not enough to enter the unique key that

BBVA sends via SMS to the telephone number validated by the customer, otherwise

that it will also be necessary for the fraudster to access the application

BBVA using a username and password. It refers to several

phishing techniques used by fraudsters such as mailing

emails impersonating BBVA, random calls, or links to

via SMS. Only when the scammers get the user and the

password to access customer accounts, then and only then

ces, the fraudster, by duplicating the SIM card, can have

have access to the accounts of those affected. Therefore, the fraudulent duplicate

dulent of the SIM card is not a necessary action (there are entities

banking. that do not send SMS with their unique keys) nor enough (they

requires access to other data and keys) to gain access to the

accounts of the affected subjects.

They clarify that with the foregoing VDF does not want to try to distract responsibility

ities or blame third parties, but simply focus the object of debate

tea. VDF may be charged with infractions only with respect to those

security measures for which it is responsible, that is, those di-

rigid to ensure that the applicant for the duplicate SIM card is

the owner of the line; they are not (nor can they be) aimed at avoiding the

identity planting (forgery of the DNI, for example) or to avoid the

access to bank accounts. through the application of the entity

credit in question.

III.- Technical and organizational measures adopted by VDF:

Difference two assumptions:

(...).

In short, it alleges that not only did it implement the security measures

to guarantee a level of security appropriate to the risk, but

which has ensured that these measures were kept up to date in

at all times, keeping out of the criminal activities carried out

by scammers and cybercriminals and trying to prevent third parties

obtain duplicate SIM cards fraudulently.

V.- The technical and organizational measures implemented by VDF are effective

and adequate to guarantee a level of security appropriate to the risk:

1. The percentage of customers that has been affected by a card change-

ta fraudulent SIM is X,XXX %; Y

2. The percentage of fraudulent SIM card changes compared to the

totality of SIM card changes made on the customer sector

individuals is X,XXX %.

VI.- We are dealing with a third party whose purpose is, through criminal activity,

go, overcome these security measures.

Access to the personal data of the interested parties (SIM card) is provided

through duly organized and plausible criminal activity.

nead. We are not facing a failure or error of the system implemented by

VDF. The capacity of these criminal organizations must be taken into account.

to adapt to the new realities and improve their methods

all to commit the frauds in question. In this sense, VDF has gone

modifying its security policy to try to anticipate new

criminal methods, although these organizations are evolving and

implementing new forms of action in order to overcome the se-

security of the operators, which makes it impossible to anticipate

tion to criminal activity in all cases.

VII.- On the alleged aspects that VDF would not have accredited:

~

~

~

Identity of the applicants of the duplicate SIM cards, in the

changes of ownership of the line or in the applicants of the copies of

invoices:

VDF has not proven the identity of the scammers and cybercriminals

because precisely these subjects have hidden their true identity

and have passed themselves off as VDF customers, overcoming through technical

nicas illicit security policies. Pretend that it proves the identity

applicants is a kind of diabolical test that is not

can require VDF.

The recordings of the telephone calls on the grounds that the

conservation periods have expired, when we find ourselves before a

total of fraudulent XXX declared in the 2019 financial year:

The Agency has not requested a copy of the recordings of the calls

phone numbers of the XXX fraudulent cases declared in 2019 by VDF,

but of the 9 cases that gave rise to the Initiation Agreement (folio 414 of the

file) and of the 20 cases reported by VDF (folio 787 of the file)

tooth). Given the above, it has not been possible to provide the recordings

of the calls because, for logistical reasons, the time during which

the recordings of said calls are stored is one month, which

It is also in accordance with the principle of limitation of the term of conservation.

vation (article 5.1 e) of the RGPD).

~

The reason why the duplicate SIM card has been sent to a

city other than that of the subscribers' residence without checks or payments.

additional guarantees" (Claimants 1, 8 and 9):

For claimant one, the SIM card change was made in

store by a commercial of the distributor ***LOCATION.3 CC Llobregat

(folio 616 of the file); and for claimant eight, it was carried out in

a store of a VDF distributor located in a Carrefour center in

Valencia (folio 878 of the file). As regards the party claiming

nine, as is shown on folios 881 et seq.

following the file, a duplicate of the card was not sent

SIM to the scammer.

The effectiveness of the "victim of fraud" check:

~

For claimant two, as can be seen from folios 603

and 604 of the proceedings, a first fraudulent duplicate of the

the SIM card on November 1, 2019, being unsuccessful the

subsequent fraudulent duplication attempts (November 4 and 5

2019) for having been marked as a "victim of fraud.

For claimant four, as can be seen from folio 605

of the proceedings, a first fraudulent duplicate of the tar-

SIM card on November 12, 2019, being unsuccessful the subsequent

fraudulent duplicate attempt (dated November 14, 2019) for ha-

been marked as a "victim of fraud."

The effectiveness of the telephone activation procedure after the

collection of the SIM card in person:

(...).

The effectiveness of multichannel care established by the face-to-face route

as a priority channel for requesting SIM duplicates, indi-

Sending the managers who attend the calls that refer to the store to

Applicants requesting the duplicate by telephone (...):

~

~

(...).

Second.- Subsidiarily, and in the event that the Agency understood that VDF

has infringed articles 5.1 f) and 5.2 of the RGPD, the existence cannot be appreciated

of guilt in the imputed infractions and, consequently, cannot impose

incur any penalty.

I.- VDF has not acted negligently, therefore the imposition of

any penalty.

Article 28.1 of Law 40/2015, of October 1, regulates the principle of guilt-

bility. Continuing with the interpretation made by the Supreme Court, to

exculpation will not suffice the invocation of the absence of guilt, but it will be

It is necessary that the diligence that was required by the person who claims his

inexistence (among others, the Judgment of the Supreme Court of January 23,

1998 [RJ 1998\601]).

Likewise, the National High Court has understood, in cases similar to the present one,

in which a third party has accessed, through criminal activities, data from

the interested parties guarded by a person in charge of the treatment, who impute ta-

made to the person responsible for the treatment could lead to the violation of the

guilt principle. By way of example, the SAN (SCA, Section 1) of 25

February 2010 [JUR 2010/82723].

Thus, even when article 9 of the LOPD establishes an obligation of result-

do, consisting of adopting the necessary measures to prevent the

data is lost, misplaced or ends up in the hands of third parties, such obligation does not

it is absolute and cannot cover a case like the one analyzed. In the case of

cars, the result is a consequence of an intrusion activity, not covered

by legal order and in that sense illegal, of a third party with high co-

computer technical knowledge that breaking security systems

established users access the database of registered users at www.porta-

latino.com, downloading a copy of it. And such facts cannot

imputed to the appellant entity because, otherwise, the principle of

of guilt". (emphasis is from VDF).

In no case can the duplication of the SIM cards of certain clients

to suppose the consideration that VDF has acted negligently. Indeed,

all its actions have always been aimed at the establishment

and supervision of technical and organizational measures aimed at guaranteeing the safety

security of your customers' personal data: design of security policies

that are followed by the after-sales service and are appropriate to guarantee

set a level of security appropriate to the risk" since "only" X.XXX % of the

clients have been victims of this type of criminal action; Update of

security measures -since May 30, 2019, it is mandatory

to make and keep a copy of the applicant's DNI - and has sent many

announcements and alerts to your stores; In those cases in which the activity of the

fraudster manages to defraud the system implemented by VDF, has reacted

do directing its actions towards 4 fronts:

.- the client: blocking the SIM card and restricting the reception of

SMS, contact and subscription of the calls operated by the scammer

.- to agents and employees: sending periodic communications with

alerts and applying penalties

.- with the State Security Forces and Bodies: collaborating in

the fight against this fraud

.-to third parties: such as credit institutions developing future tools

such as (...).

Consequently, it has acted with the due diligence that is required and in accordance with

The sanctioning law provides me, the imposition of any sanction is not appropriate.

na.

II.- In any case, the identity theft of those affected is de-

due to the existence of human errors, which are inevitable and on which

VDF cannot have effective control:

In these (residual) assumptions, we would be facing human errors in which

the scammer or cybercriminal, using tricks and using in his favor

his criminal experience, has managed to circumvent security policies, provoking

do the human error of the after-sales service.

The Agency has ruled on numerous occasions on human errors

hands, emphasizing that they cannot be punished. For example in

Sanctioning Procedure PS/00210/2019 and in Procedure E/

02877/2019, citing the SAN (SCA, Section 1) of December 23

2013 [JUR 2014\15015]: "The issue, therefore, must be resolved in accordance with

the principles of punitive law since mere human error does not

can give rise, by itself (and especially when it occurs with a

isolated), to the attribution of sanctioning consequences; well, to be done

thus, a system of strict liability would be incurred that is prohibited by our

constitutional order".

Third.- Subsidiarily, and in the event that the Agency understands that there has been

infringement has occurred and a sanction must be imposed, the following must be taken into account:

following aggravating and mitigating circumstances:

VDF respectfully disagrees with the aggravating factors listed in the Initiation Agreement:

The nature, seriousness and duration of the offence, taking into account the nature

nature, the scope or purpose of the treatment operation in question, as well as

the number of interested parties affected and the level of damages that they have

suffered:

I. Nature, seriousness and duration of the infraction:

The only personal data on which the disposition is lost (temporarily,

until the new SIM is locked) is the phone line. The loss of dis-

position and control over other personal data (such as name, surname,

DNI, address, bank details) occurs:

(i) either at a time prior to VDF's participation (for example, re-

laxation of human behavior in the provision of certain data to later

acquaintances, who obtain them through phishing or "engineering" practices.

social river").

(ii) either at a time after your participation (for example, use

SMS to send access codes to electronic banking), for

what cannot be blamed.

The events occur in a period of less than one year, not more than as indicated

the agency.

The nature of the facts makes it very difficult -almost impossible- to completely eradicate

complete these practices, so the temporary element cannot be taken into account.

counts as an aggravating circumstance, even more so when VDF has implemented a policy of

security aimed at preventing this type of behavior.

- Number of stakeholders affected:

The percentage of customers who have been affected by a fraudulent change of

SIM card is X.XXX %, and that the percentage of fraudulent card changes

compared to the total number of SIM card changes made on

in the private customer sector is X.XXX%, so we understand

that the number of stakeholders affected is not high when compared to the number

number of potential affected.

- Level of damages suffered:

The Agency emphasizes that by controlling the subscriber's line it is possible to

have access to the "SMS addressed to the legitimate subscriber to carry out operations

online transactions with banking entities supplanting their identity". In this sense,

do, the identity verification system used by a bank

(for example, sending SMS with access codes) responds to the will of

the credit institution and the user, not VDF. In other words, the old risk

ne generated by the credit institution when using this verification system of

the identity of the interested party, not by VDF.

Also, another element to take into account is that the bank reimburses

the amounts defrauded from the victim of the fraud, as highlighted by BBVA

in the response to the request for information from the Agency contained in the folio

292 of the file: "[...] returning the amounts of the fraudulent operations

slow as well as the commissions generated".

II. The intentionality or negligence in the infringement:

It is completely ruled out. VDF has indeed ensured a procedure that

guarantees the protection of the personal data of its clients (that is, their tar-

SIM card). A good example of this is that only X.XXX % of customers

have been affected by this scam and has also carried out actions

Please keep this security policy up-to-date.

III. Any measure taken by the data controller to alleviate the damage

damages suffered by the interested parties:

(...).

IV. The degree of responsibility, taking into account the technical or organizational measures

have applied under articles 25 and 32 of the RGP: it has implemented

take appropriate technical and organizational measures for the risk generated, that is,

tending to ensure that whoever requests the duplication or change of a SIM card is

the line owner.

V. Any previous infraction committed by the data controller: Until the fe-

cha, VDF has not been sanctioned for infringement of articles 5.1 f) and 5.2 of the RGPD

in relation to similar facts, a circumstance that must also be taken into account.

account to modulate the sanction downwards.

SAW. The degree of cooperation with the supervisory authority in order to remedy

to the infringement and mitigate the possible adverse effects of the infringement: the degree of

cooperation with the Agency has been high.

VII. The categories of personal data affected by the infringement: They allege that

the affected personal data cannot be considered as circumstance

aggravating. The Agency commits an error of assessment, insofar as the

identity theft is prior to the issuance of the duplicate SIM card. The

overcoming security policies, it can be a means used together with others,

to circumvent the identity controls implemented by other economic operators.

economic, but has nothing to do with the activity with respect to which it is required to

VDF in the adoption of adequate security measures. In fact, it will depend on

security systems implemented by banks. the fact of

that the fraudster may or may not access the accounts of the affected party, not being able to

hold VDF responsible for the lack of robustness of the security system of a terminal

zero (the bank entity).

VII. Any other aggravating or mitigating factor applicable to the circumstances of the

case, such as financial benefits obtained or losses avoided, directly or

indirectly, through infringement: Criminal activity has also involved

a reputational damage to VDF and a fraud of its security policies.

dad.

IX. The continuing nature of the infraction: It is postulated in favor of the criterion of the Agency

cia that considers that these infractions do not have a continuous character.

Fourth.- Evidence that this party deems appropriate to propose:

(...).

TWENTIETH: Dated April 14, 2021, after verifying that it was not attached

part of the documentation that indicated having provided, VDF is required to

within 10 days from the day following your notification, provide the following

documents:

(...).

Said requirement was notified on April 19, 2021, through the Service

of Electronic Notifications and Authorized Electronic Address, according to the certificate that

appears in the file.

TWENTY-FIRST: In response to said request for information, dated

April 29, 2021, VDF sends the requested documentation.

TWENTY-SECOND: On April 30, 2021, the instructor of the

procedure agrees on the opening of a period of practical evidence in the

following terms:

“The claims filed by

A.A.A.; B.B.B.; C.C.C.; F.F.F.; G.G.G.; K.K.K.; L.L.L.; Ñ.Ñ.Ñ.; and O.O.O., and his do-

documentation. The documents obtained and generated by the Inspection Services

before VODAFONE ESPAÑA, S.A.U, and the Report on previous actions of

Inspection that are part of file E/11418/2019. 2. They are also given

by reproduced for evidentiary purposes, the allegations to the initiation agreement PS/

00001/2021 filed by VODAFONE ESPAÑA, S.A.U., on March 3

of 2021 and April 29, 2021 and the documentation that accompanies them:

 Document 1, (...).

 Document 2, (...).

 Document 3, (...).

 Document 4, (...).

 Document 5, (...).

 Document 6, (...).

 Document 7, (...).”

TWENTY-THIRD: On July 28, 2021, the instructor of the procedure

formulates a Proposal for a Resolution, in which it proposes that the director of the AEPD

VODAFONE ESPAÑA, S.A.U., with CIF A80907397, is sanctioned for infraction of the

article 5.1.f) and 5.2 of the RGPD, typified in article 83.5.a) of the RGPD and in article

72.1.a) of the LOPDGDD, with an administrative fine of 4,000,000'00 (four million

ns of euros).

On August 2, 2021 through the Electronic Notification Service and

Electronic Address Enabled, the Resolution Proposal is notified.

TWENTY-FOURTH: On August 5, 2021, VDF requests the extension of the

term to formulate allegations to the Resolution Proposal.

TWENTY-FIFTH: On August 9, 2021, the Agency grants the extension

tion urged.

TWENTY SIXTH: On August 23, 2021, this Agency receives, in

time and form, written by the lawyer and representative of VDF, which proceeds to

formulate allegations to the Resolution Proposal and in which, after expressing what

to his right it was convenient, he ends up requesting, as he did in the allegations to the Agreement

beginning, the dismissal of the file with the consequent filing of the

actions since none of the imputed infractions have been committed and

subsidiarily, in case of imposing a sanction, the imposition of an amount

minimum, in light of the mitigating circumstances alleged.

As a previous allegation, VDF points out that the Resolution Proposal proposes the

imposition of a fine of 4,000,000.00 on VDF for an alleged infringement of the

article 5.1.f) and 5.2 of the RGPD, infraction classified as very serious article 83.5.a)

of the RGPD and by article 72.1 of the LOPDGDD, because VDF would have violated the

principles of integrity and confidentiality and proactive responsibility, by facilitating

SIM card duplicates to people who are not the holders of the mobile lines,

after the overcoming by these third parties of the security policies implemented by

VDF.

Likewise, it states that the sanctioning file has its origin in nine

claims filed with the Agency, although it has not only taken into account

the concrete facts and specificities that occurred in those cases, but it has

prosecuted the security measures adopted by VDF in general.

Below, and without prejudice to the fact that VDF refers in its entirety to the allegations-

tions submitted on March 3, 2021 to the Start Agreement, states that:

1). The purpose of this proceeding should be limited to determining whether VDF has adopted

taken the appropriate technical and organizational measures to avoid, to the extent possible,

possible, that duplicate SIM cards be issued to subjects who are not the holders.

rest of the mobile lines. Prosecution cannot be extended to actions

earlier and later carried out by cybercriminals. To this question of

Says the first allegation.

VDF emphasizes that this procedure must be addressed solely and exclusively to
analyze whether the technical and organizational measures adopted by VDF are appropriate
to ensure (as far as possible) that duplicate SIM cards are
provided to the holders of the telephone lines and that the adequacy or not of the me-
measures adopted by VDF cannot be made to depend on a future event that does not determine
depends on his principal, that is, that the cybercriminal manages to access the bank
online of the affected person.

two). VDF argues that it has complied with the principles of confidentiality and integrity.
responsibility and proactive responsibility, as well as the obligation to adopt the measures
appropriate technical and organizational measures: the security measures adopted by Vodafone
ne are not static, but rather have been revised and updated
do over time. The second allegation is devoted to this question.

3). The adoption of technical and organizational measures is not an absolute obligation:
the figures in the file are a relevant indication that VDF has complied
with the principle of integrity and confidentiality. It is to this question that the allegation
third.

In support of this allegation, VDF indicates that the figures in the file de-
show that you have complied with the principle of integrity and confidentiality; fencing-
used as arguments that VDF has proceeded to the implementation of objective measures
mind suitable to protect the integrity and confidentiality of personal data
of clients taking into account the number of cases in which said security measures

security have been exceeded, taking as a reference the time period in which

that the facts that are the object of these proceedings are framed, that is, from the

July 29, 2019 (case of Claimant 5, folio 109 of the file) until July 2,

2020 (case of Claimant 8, folio 450 of the file), we see that Vodafone

has rejected a total of XXXX requests for duplicate SIM cards, avoiding

potential fraud problems and XXX cases have materialized, which demonstrates

It would seem that the implemented security measures work, according to VDF.

4). Subsidiarily, in the event that it is understood that there has been an infringement,

There are several factors that lead to the conclusion that the actions of VDF

has not been negligent and, consequently, cannot be imposed to the same sanction al-

guna. The fourth allegation is devoted to this question.

Arguing in his defense that in the present sanctioning procedure they have evaluated

Evaluated the circumstances of nine specific cases; that the figures in the experience

tooth (which have not been discussed by the Agency) show that we are

in isolated cases, from which it can be inferred that VDF's actions have not been

negligent; for all the measures taken by VDF to prevent duplicate fraud.

card dulent; conducting criminal activities of third parties to access

certain personal data of those affected; and finally the existence of errors

that have led to the issuance of the fraudulent duplicates.

5). VDF states that subsidiarily to point 4) above, in the event that

understood that a sanction can be imposed, the circumstances must be taken into account.

circumstances identified in the fifth allegation to reduce the amount of the penalty

tion.

Stating in this allegation that subsidiarily, in the event that the

Agency understood that there has been an infraction and that the im-

position of a sanction against Vodafone, its principal considers that, being the same

disproportionate (a penalty of approximately XXX.XXX euros is proposed for

each case), it must be modulated downwards according to the circumstances that are exposed.

nen in his allegation.

These circumstances are the aggravating circumstances taken into account by the AEPD, and which are the

following:

Nature, seriousness and duration of the infringement (article 83.2 a) of the RGPD):

party in relation to the time period with respect to which the events take place, that the

The Agency alleges that after June 2, 2020 (the date on which the

the last of the nine claims that have given rise to this file) was

three additional claims were filed denouncing similar facts that

have not been subject to accumulation in this sanctioning procedure and that they do not

should be taken into account as aggravating factors.

Number of interested parties affected (article 83.2 a) of the RGPD): states that, the

XXX cases cannot be taken into account without putting them in their proper context al-

gaining a series of circumstances, in relation to the total number of VDF clients, with the

total requests for duplicate SIM cards and with the number of card requests

SIM cards denied.

Level of the damages suffered (article 83.2 a) of the RGPD the degree of responsibility

liability that, in its case, can be attributed to VDF, cannot be made to depend on

an action by a third party that is beyond the control of my principal, that is: the measures

security measures implemented by one or another banking entity or even the fact

whether or not the affected party has electronic banking.

Intentionality or negligence in the infringement (article 83.2 b) of the RGPD): Manifest

VDF that in order to avoid unnecessary repetition, refers to the Fourth Allegation in

regarding the absence of negligence. And he also adds his disagreement with the following

following statement from the Agency: "Similarly, the fact that VDF has implemented

subsequently made changes to the existing technical or organizational measures.

test, corroborates that those others did not provide adequate security" and that they did not

the fact of complying with the RGPD, which im-

puts a continuous and systematic evaluation of the security measures to be adapted

subjecting them to changing risks, an issue that has been dealt with in the Second Allegation

second of this writing. If the sanction is imposed for the lack of, in the opinion of the Agency,

due diligence, the negligence that precisely constitutes the infringing act

can, in turn, be valued as an aggravating circumstance.

About the measures taken by the person in charge (article 83.2 c) of the RGPD): Argument-

ta VDF that the Agency refers to the adoption of a list of measures (the list of

measures are those expressly stated by VDF in section III of the Allegation

Third statement of his pleadings brief to the Agreement to initiate this proceeding.

ment, this allegation, like the rest of the allegations to the aforementioned Agreement, were

duly answered in the Fourth Legal Basis of the Proposal for Re-

solution, regarding which he makes two clarifications:

The first precision relative to the fact that VDF has also adopted many other measures

you give.

The second precision, it is admitted that the subsequent measures adopted have the consi-

deduction of minimums.

Degree of responsibility of the person in charge (article 83.2 d) of the RGPD): Indicates VDF that, as stated in the Second and Third Arguments of this writing, VDF has implemented adequate technical and organizational measures for the risk generated generated by my client, that is, tending to ensure that whoever requests the duplicate or change of a SIM card is the owner of the line. We refer to said allegations tions to avoid unnecessary repetition.

Previous violations of the Initiation Agreement committed by VDF (article 83.2 e) of the RGPD): VDF argues that this point was not included by the Agency as circum- aggravating substance in the Agreement to Start the sanctioning procedure of February 8- 2021 (the "Startup Agreement") showing its disagreement with this fact because- which was included as an aggravating circumstance when Vodafone included in its Allegation Brief March 3 a reference to the fact that Vodafone had not been sanctioned for in- fraction of articles 5.1 f) and 5.2 of the RGPD in relation to facts similar to those treated in this file and that the infractions and because none of the eleven sanctioning resolutions cited by the Agency in its Resolution Proposal- tion refers to infringements of articles 5.1 f) and 5.2 of the RGPD in relation to he- facts similar to those dealt with in this file.

Categories of personal data affected (article 83.2 g) of the RGPD): According to VDF the Agency understands that the infraction in question "enables the theft of identi- dad." In addition, in its defense VDF refers to the allegations contained in its pleadings brief dated March 3, 2021.

Linking the activity of the offender with the performance of data processing of personal nature (article 76.2 b) of the LOPD): the Agency refers to the fact that the "number

of mobile telephone lines [...] positions VDF as one of the telephony operators

largest communications in our country.

6). Finally, it states that in the Sixth Argument it lists the new evidence of

those that are intended to be worth; requests the evidence that it deems convenient to propose, which is

are presented as supporting documents of lack of guilt, or,

where appropriate, the sanction proposed by the Agency, documents 1 and

2 provided: Document 1 copy of the email sent by VDF to the respondents

agency notices on June 7, 2019 regarding SIM card duplicates

by telephone and Document 2 copy of the letter from the Provincial Police Brigade

Court of Valladolid (Technological Research Group), in which you can observe

It should be noted that the State Security Forces and Bodies have congratulated VDF for its

collaboration on different occasions.

These Allegations will be answered in the Law Foundations of the

this Resolution.

Of the actions carried out in this procedure and the documentation

in the file, the following have been accredited

PROVEN FACTS

FIRST: VDF is responsible for the data processing referred to in the presentation.

the Resolution Proposal, since according to the definition of article 4.7 of the

RGPD is who determines the purpose and means of the treatments carried out with the

purposes indicated in its Privacy Policy: offer service (process orders and

provide products and services, billing and customer service, information message

mation of services, providing roaming services); improve the service (innovate

products and services, manage their networks and understand network usage); marketing and

adapting its service to customer needs (online advertising, research,

tion and analysis); o profiling (credit analysis and identity verification)

ity, fraud prevention and security).

SECOND: VDF has a specific Security Policy for the change of

SIM that you carry out through (...).

The request for a duplicate by the client can be made:

(...).

THIRD: VDF has defined in the (...) the following contractual clauses:

(...).

FOURTH: VDF sent up to (…).

FIFTH: VDF sent (...).

SIXTH: On September 2, 2019, this Agency received a claim

mation made by claimant one (file with reference no.

E/10004/2019), directed against VDF, after running out of network on the line ***TELÉFONO.1,

on August 5, 2019, without being able to receive or make calls.

VDF, on August 5, 2019, made a duplicate of the corresponding SIM card.

tooth to the ***TELEPHONE.1 line at 8:39 p.m., which was delivered to a third

person at the VDF store in the ***CENTRO.1 shopping center (Barcelona).

There is an invoice number ***FACTURA.1 issued on August 7, 2019, which

contains the charge corresponding to the issuance of the SIM card, where it specifies

as a delivery address a Shopping Center located in the municipality of

*** LOCATION.2, when the claimant party has his habitual residence in the

municipality of *** PROVINCE.1.

For these facts, the claimant one filed a complaint with the Civil Guard

of ***LOCALIDAD.1 (***PROVINCIA.1), on August 7, 2019, with number

of affidavit ***ATESTADO.1 in which it states that on August 6, after

get a duplicate SIM card, he received a series of SMS from Banco Santan-

der informing you about making a transfer from online banking. To the

going to his bank, he was informed of the completion of a total of 25 operations of

expenses, including: a loan amounting to 5,690.76 euros, the provision of two

credit cards with a balance of 5,000.00 and 1,000.00 euros respectively, and the

subscription of an insurance linked to the loan for an amount of 806.66 euros.

In relation to this claim, VDF informed this Agency that, on the 5th of

August 2019, a change of SIM card was made in store by a commercial of the

distributor *** LOCATION.3 CC Llobregat and that processed the file as a service

Fraudulent deal, blocking the duplicate SIM card object of the claim on date 6

August 2019.

Indicates that prior to the request to change the SIM there is a call to the

customer service, where after passing security policy, the duplicate of

two invoices, it is confirmed that the number originating the call is a mobile line that

does not belong to the client and is hosted on another operator's network.

VDF has not provided a copy of the ID of the applicant for the duplicate, indicating that it was requested

He sent the documentation to the distributor in order to confirm if he had followed the process of

documentation custody. (...).

SEVENTH: On November 20, 2019, this Agency received a re-

claim made by claimant two (file with reference no.

E/12065/2019), directed against VDF, after running out of service on line XXXXXXX-

XX on November 4 and 12, 2019, and issue three duplicates of your card

SIM in favor of third parties, without their consent.

Due to these facts, the claimant party two, presented three complaints with number of

certified ***CERTIFICATE.2 dated November 4, 2019; ***ATTESTED.3 of

dated November 5, 2019; and, ***ATESTADO.4 dated November 12, 2019;

all of them, presented before the DGPN in the Madrid-San Blas offices.

He states that he was able to verify through his laptop that in the account of

the ING entity in which it appeared as authorized, had returned four receipts and

they had made a cashier draw of 890.00 euros.

In person at a VDF store, he was informed that, on November 4, 2019,

an unknown person had requested a duplicate of his SIM card online through

see email ***EMAIL.3. As of November 5, 2019, check

a series of unauthorized charges through a BANKIA Visa credit card,

as well as three transfers received in the ING account in which it appears as auto-

curly, for amounts of 3,000.00, 6,000.00 and 2,500.00 euros. On November 12-

bre 2019, again, you run out of service on your mobile device. contact with

VDF and inform him that unknown persons had canceled his SIM card and made

They had made a duplicate online.

In relation to this claim, VDF informed this Agency that three

SIM card duplicates:

 The first, dated 11/1/2019 at 23:23:22 (...). The request to change

SIM is made from a call to customer service from numbers

hidden river.

 The second, dated 11/4/2019 6:30:23 by (...) using the SIM card

***SIM.9.

 The third dated 11/12/2019 11:58:03 by (...), using the SIM card

5***SIM.10.

It states that the second and third duplicates were unsuccessful because they were

marked the client as a "victim of fraud". (...).

EIGHTH: On November 28, 2019, this Agency received a re-

claim made by the representative of claimant three (file with

no. reference E/00557/2020), directed against VDF, after being requested by a third party and

issue in your favor, dated September 28, 2019, a duplicate of the card

SIM of the line number ***PHONE.14 of which her husband was the holder.

Due to these facts, the daughter of claimant three filed two complaints with

certificate number ***ATESTADO.5, dated October 24, 2019 and

***ATESTADO.6, dated November 4, 2019 before the DGPN in the

dependencies of ***LOCALITY. It manifests in the complaints, that in the bank account

ING company owned by their parents, two loans were requested

personal for a value of 23,000.00 and 3,000.00 euros and two withdrawals were made

at the ATM for a value of 2,000.00 and 3,000.00 euros. 5,000.00 were also transferred

euros to a Banco Santander account owned by claimant three.

Several cash withdrawals were made in the destination account through Bizum,

as well as purchases with Wallet Santander, movements with the card and sale of shares.

nes. An investment fund was also sold for a value of 5,000.00 euros, reimbursement

using the money in his father's account.

In relation to this claim, VDF informed this Agency that (...).

NINTH: On November 28, 2019, this Agency received a re-

claim made by claimant four (file with number of

reference E/00558/2020), directed against VDF, after being issued on the 12th and 14th of

November 2019 two duplicates of the SIM card of the lines ***TELÉFONO.15 and

***TELEPHONE.3 by telephone, in favor of a third party other than the owner of the lines.

On November 12, 2019, from your checking account and through the bank to

distance, four transfers were made, without your consent:

Concept

Cash withdrawal without support

Transfers XXXXXX

Transfers XXXXXX

Transfers XXXXXX

Date

12-11-2019

12-11-2019

12-11-2019

12-11-2019

Amount

300.00

900.90

779.90

810.90

It is proven that BBVA reimbursed the total of the amounts stolen.

Due to these facts, the wife of claimant four filed a complaint with

certificate number ***ATESTADO.6, dated November 13, 2019, before the

Command of the Civil Guard of Madrid Company of ***LOCALITY.

In relation to this claim, VDF informed this Agency that a first

first fraudulent duplicate of the SIM card on November 12, 2019, resulting in in-

The subsequent attempt on November 14, 2019 was successful, as the

customer as a "victim of fraud".

VDF reported that (…).

TENTH: On December 4, 2019, this Agency received a claim

mation made by the complaining party five (file with reference number E/

00559/2020), directed against VDF, after losing service on the ***TELÉ-

FONO.4, dated July 29, 2019.

On this last date, it was issued in favor of a third person other than the holder of the

line, a duplicate of the SIM card in the store located in Avd. Sweden of Santa Cruz

de Tenerife, when claimant five is domiciled in Barcelona.

On July 29, 2019, from his checking account, two transfers were made

tions in favor of J.J.J., without his consent:

Concept

Purchase order

Purchase order

Date

07-29-2019

07-29-2019

Amount

2,175.00

2,713.00

Due to these facts, claimant five, filed a complaint, on the 5th of

August 2019, with procedure number: ***DILIGENCIA.1 before the Mossos

d'Esquadra, OAC of ***LOCATION (Girona).

In relation to this claim, VDF informed this Agency that it was carried out, in fe-

cha July 29, 2019, from a physical store of a distributor, specifically, in

Santa Cruz de Tenerife, a change of the SIM card corresponding to the line ***TE-

LÉFONO.4, whose owner is the claimant party five. Specifically, there is the change of

numbering of the original SIM card "***SIM.6" to the number "***SIM.7" ("(…)").

Likewise, it was verified that on July 30, 2019, the management of another

change of SIM linked to the same mobile line, carried out, in the same physical store

of VDF. In particular, there is the change of the SIM Bis to the numbering "***SIM.8"

("(…)").

He states that until November 29, 2019, he had no record of the fraud nature

dulent of the processing of SIM changes made on July 29 and 30

of 2019, despite the fact that, as a result of what happened, the claimant party five, filed in

the month of August 2019 a total of 3 claims:

~

~

The first, with no. XXXXXXX before the Fraud Department, requesting

the application of a more restrictive security policy.

The second with no. XXXXXXX, before the Customer Service Department,

requesting the application of a security key.

- And the third, with no. XXXXXXX, in which he reiterates his requests for a

security key and a more restrictive policy.

Likewise, the claimant party five, filed a claim with the SETSI

requesting compensation for damages, obtaining a response

refusal by VDF, which was not considered responsible for the transactions

bank transactions made fraudulently, after exceeding the third person, in both

cases, the security policy.

VDF has not contributed (...).

ELEVEN: On February 17, 2020, this Agency received a re-

claim made by claimant six (file with reference no.

E/03065/2020), directed against VDF, after running out of service on the line

***TELEPHONE.7, dated January 7, 2020.

Two days before, that is, on January 5, 2020, VDF sent to an email address

electronic ***EMAIL.1 -address that did not appear in the personal data of the

client-, a duplicate of an invoice, to a third person other than the holder of the

nea, who made up to thirteen calls to Customer Service, becoming

go through this It consists (...).

Due to these facts, claimant six filed a complaint, on the 9th of

January 2020, with procedure number ***DILIGENCIA.2 before the Mossos

d'Esquadra USC of ***LOCATION (Barcelona). Reported receiving an SMS

from ING informing him that someone had tried to access his

It has your ID number.

In relation to this claim, VDF informed this Agency that (...).

TWELFTH: On March 17, 2020, this Agency received a re-

claim made by the claimant seven (file with reference no.

E/03632/2020), directed against VDF, in relation to the lines ***TELÉFONO.11,

***TELEPHONE.16 and ***TELEPHONE.17, after being accepted on December 15,

2019, a change of ownership in the services attached to these lines, in favor of a

third person. Likewise, on January 4, 2020, it was left without service in the

line ***PHONE.11.

On this last date, there are 5 fraudulent charges made in the checking account

that he shares with his wife, amounting to a total of 7,740.00 euros and two charges

made through the credit card amounting to 2,269.40 euros.

Concept

Lottery payment Manises

Lottery payment Manises

cashier layout

cashier layout

cashier layout

Date

04-01-2020

04-01-2020

04-01-2020

04-01-2020

04-01-2020

Amount

1,500.00

240.00

1,000.00

2,000.00

2,000.00

Due to these facts, claimant seven filed a complaint, on the 4th of

January 2020, before the DGPN in the offices of ***LOCALIDAD, with number of

attested ***ATESTATED.7. He stated that he had received a message from his bank ING indicating

when they had canceled his PIN code and then he was left without coverage. After

getting through to VDF discovered that his SIM card had been duplicated.

In relation to this claim, VDF informed this Agency that there was a change

title deed that associated the data of a third party, Mr. M.M.M., to the ID ***ID.1 of the claim.

keep. Subsequently, a second owner change took place that associated the ID of

previous client to the data of another third party, D. N.N.N. It also confirms that on the date

January 4, 2020, a SIM change was processed on the line ***TELÉFONO.11,

associated with the ID ***ID.1. This change of SIM was managed in person, through

you see (…).

Claimant seven is domiciled at *** LOCATION.

VDF has not contributed (...).

THIRTEENTH: On June 30, 2020, he entered this Agency

a claim made by the claimant party eight (file with number of

reference E/08544/2020), directed against VDF, after running out of service on the line

***PHONE.12, dated June 2, 2020.

On that same date, VDF processed a modification order on the services associated

ciated to the client ID ***PHONE.13, of which the claimant eight was the owner,

in order to modify the services VDF One Fibra 50Mb + M + TV + Total + Fixed for the rate

fa VDF One Unlimited Total Fiber 1Gb, at the request of a third party other than the

complaining party eight.

Claimant eight is domiciled in Seville, however, both the duplicate

of the SIM as the modification order on the services associated with its ID, it is carried out

made at the point of sale (...) ***LOCALITY (Valencia) in favor of a third party

na, other than claimant eight.

The Mobile, Broadband, Landline and TV Service Contract for Private Customers for the

that the modification of the contracted services materializes is not signed by

any client (neither by the owner of the line, nor by a third person on their behalf).

On June 2, 2020, an immediate transfer is made in favor of Q.Q.Q.

for an amount of 3,506.00 euros from the current account of the claimant party eight.

Likewise, a series of charges are made on the Visa/MasterCard credit card of

which is the owner, between June 2 and 4, 2020, for the following concepts:

Concept

Mobile payment in Soloptical Gran, Valencia

Mobile payment in Mezea M3, Chirivella

Mobile payment in El Rinconet, Alfafar

Reimbursement, Sedaví

Mobile payment in tobacconist, Valencia

Reimbursement, Valencia

Reimbursement, Valencia

Reimbursement, Valencia

Mobile payment in El Corte Inglés, Valencia

Mobile payment in El Corte Inglés, Valencia

Mobile payment in El Corte Inglés, Valencia

Mobile payment in El Corte Inglés, Valencia

Mobile payment in El Corte Inglés, Valencia

Mobile payment in Cortefiel, Valencia

Mobile payment in Supermoments, Valencia

Date

2-06-2020

2-06-2020

2-06-2020

2-06-2020

3-06-2020

3-06-2020

3-06-2020

3-06-2020

3-06-2020

3-06-2020

3-06-2020

3-06-2020

3-06-2020

3-06-2020

3-06-2020

Amount

292.50

1,661.60

1.20

300.00

141.00

900.00

1,000.00

1,000.00

17.45

24.45

20.95

24.45

809.00

104.85

110.85

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

51/88

Mobile payment in Turmalina, Valencia

Mobile payment in Druni, Torrent

Mobile payment in Antonio Jewelry, Torrent

Mobile payment in Primera Ópticas, Torrent

Mobile payment in Estanco, Valencia

Mobile payment in Estanco, Valencia

Carrefour Saler, Valencia

Carrefour Turia, Xirivella

3-06-2020

3-06-2020

3-06-2020

3-06-2020

3-06-2020

3-06-2020

4-06-2020

4-06-2020

1698.00

724.29

1,833.00

175.80

150.00

138.00

1,566.00

1,566.00

In relation to this claim, VDF informed this Agency that, on July 2,

In January 2020, a SIM change was processed on the ***TELÉFONO.12 line. Saying

change was managed in person, through the VDF Point of Sale operated

by (...), located in *** LOCATION (Valencia), after overcoming the security policy

of VDF. On June 3, 2020, he processed a new SIM change, in order to

cancel the change made on June 2, reestablishing for this purpose the line

***TELEPHONE.12 and its control and interrupt the process of activating the rates with-

treated.

VDF has not provided a copy of the DNI or identification document collected in the contract.

presence, alleging that it is the points of sale that carry out the verification and

a copy of the identification documents and that it no longer maintains a contractual relationship with

the distributor. Nor does it provide the identification document collected in the application for

SIM duplication.

FOURTEENTH: On June 8, 2020, this Agency entered a

claim made by the claimant nine (file with number of

reference E/05287/2020) directed against VDF, after running out of service on the line

***TELEPHONE.13, on January 7, 2020 and two changes in title were authorized.

authority of your line, without your consent.

There is invoice number ***FACTURA.3 issued by VDF on the same date, which

contains the charge corresponding to the issuance of the SIM card, where it specifies

as delivery address XXXXXXXXX in the municipality of *** LOCATION (Girona),

when the claimant nine, has his habitual residence in the municipality of

***LOCALITY (Las Palmas).

Due to these facts, on January 7, 2020, he filed a complaint with number

of attested ***ATESTADO.8 before the DGPN in the dependencies of ***LOCALITY.

He states that after losing the line, he received confirmation through his company's Wi-Fi

mation of an operation, being able to verify through an email a loan of

7,000.00 euros and three cash withdrawals for the following amounts: 2,000.00,

2,000.00 and 1,000.00 euros, as well as an internal transfer of 4,000.00 euros.

Likewise, there is a claim addressed to Customer Service, dated 8

January 2020, requesting information on the two changes of ownership and the

issuance of a SIM card, without your consent.

In relation to the filed claim, VDF informed this Agency that, with fe-

On January 7, 2020, there were two changes of ownership of the ID ***ID.2,

ownership of the claimant nine, in favor of third parties. First,

there was a change of ownership that associated the data of a third party, Mr. M.M.M. to ID

***ID.2 of the claimant. Subsequently, a second change of head took place

associated the previous client ID with the data of another person, Mr. XXXXXX. Likewise,

has also been able to verify that on January 7, 2020, a change of

SIM on the line ***PHONE.13, associated with the previous ID. Said SIM change was

managed in person (...). On January 9, 2020, after having

proof of the facts object of the claim, and after verifying that it was before management

statements that, despite having the appearance of being truthful, were of a fraudulent nature, proceeding

gave to block the client's account, restricting the use of the services associated with the

ID ***ID.2.

VDF has not contributed (...).

FIFTEENTH: VDF has subsequently carried out measures and developed

action plans to prevent duplicate SIM card fraud, which focuses

in four lines of action:

(...).

SIXTEENTH: In the reference time period in which the events are framed,

the object of these proceedings, that is, since July 29, 2019 (case

Claimant 5, folio 109 of the file) until June 2, 2020 (case of Claimant 5, folio 109 of the file)

claimant 8, folio 450 of the file), VDF states that (...).

FOUNDATIONS OF LAW

FIRST: Competition.

By virtue of the powers that article 58.2 of the RGPD recognizes to each Authority of
Control, and according to what is established in articles 47, 48, 64.2 and 68.1 of the LOPDGDD, the
Director of the AEPD is competent to initiate and resolve this procedure.

In initiating the sanctioning procedure, the AEPD has acted in accordance with the
general principles of article 3.1 of the LRJSP, among which is the service
citizens, good faith, legitimate expectations or transparency of the
administrative action.

The AEPD has attributed a series of competencies, powers and functions provided for in
Articles 55 and following of the RGPD that according to article 8 of the LRJSP,
They are inalienable and will be exercised by the administrative bodies that have them attributed.
taken as their own.

In the exercise of the functions and powers attributed to it by articles 57 and 58 of the
RGPD, controls the application of the RGPD, conducts investigations and imposes, where appropriate,
administrative sanctions which may include administrative fines, and
orders the corresponding corrective measures, according to the circumstances of each
particular case. Thus, you can carry out the investigations you deem appropriate (ar-
Article 67 of the LOPDGDD), after which you can decide to initiate an ex officio procedure
sanctioning party (article 68 LOPDGDD).

In the case examined, the investigations carried out in order to determine the co-
mission of some facts and the scope of these revealed a possible lack
of security measures.

SECOND: Applicable regulations.

Article 63.2 of the LOPDGDD determines that: "The procedures processed by the Spanish Data Protection Agency shall be governed by the provisions of the Regulations to (EU) 2016/679, in this organic law, by the regulatory provisions dictated in its development and, as long as they do not contradict them, on a subsidiary basis, by the general rules on administrative procedures."

THIRD: Violation.

The actions outlined in the Background have been aimed at analyzing the procedures followed to manage SIM change requests by VDF, identifying the vulnerabilities that could exist in the operational procedures implanted, to detect the causes for which it could be producing ing these cases, as well as finding points of non-compliance, improvement or adjustment, to determine responsibilities, reduce risks and increase safety in the workplace. treatment of the personal data of the affected persons.

The previously declared proven facts violate article 5.1.f) and article 5.2 of the RGPD and are constitutive of the infraction foreseen in article 83.5.a) of the RGPD that considers a very serious infringement the violation of: "the basic principles for treatment, including the conditions for consent under the ar- Articles 5, 6, 7 and 9," typified with an administrative fine of 20,000,000.00 euros. maximum or, in the case of a company, an amount equivalent to 4% as a maximum of the total global annual turnover of the previous financial year higher, opting for the highest amount.

They are also constitutive of the infraction typified in article 72.1.a) of the LO- PDGDD that considers a very serious infraction for the purposes of the prescription: "The treat-

processing of personal data violating the principles and guarantees established in the

Article 5 of Regulation (EU) 2016/679".

Article 75 of the LPACAP refers to the "Instruction Acts" as those necessitated

necessary for the determination, knowledge and verification of the facts under

of which the resolution must be pronounced. Well, the instruction resulted after

the analysis of the evidence practiced and the allegations adduced in accordance with the

seen in articles 76 and 77 of the LPACAP, that VDF despite having a document

document called security policy that contained the security measures that

should be adopted in the processing of personal data necessary for the provision

provision of the contracted services and throughout their life cycle, these measures have

clearly insufficient result.

From the analysis of the procedures followed by VDF -documented with the claims-

tions and the additional cases studied -, the following facts of interest result:

VDF has not been able to prove:

~

~

~

~

The identity of the requesters of the SIM card duplicates.

The identity of the applicants in the changes of ownership of the line.

The identity of the requesters of the copies of the invoices.

Recordings of telephone calls on the grounds that the deadlines

of conservation have expired, when we find ourselves before a total of XXX

fraudulent declared in the year 2019.

~

~

The reason why the duplicate SIM card has been sent to a city

different from the residence of the subscribers without controls or additional guarantees.

final (claimant parties cases: ONE, EIGHT and NINE).

The effectiveness of the “Victim of fraud” check, which shows an impairment in

the resilience of treatment systems and services, since it is not guaranteed

sufficient speed or traceability of information in adverse conditions.

such as those that occur in the cases analyzed.

The effectiveness of the telephone activation procedure after collection

give the SIM card in person.

The effectiveness of multichannel care that establishes the face-to-face route as

priority channel for requesting SIM duplicates, indicating to managers

agents who attend the calls that refer to the store the applicants who request

They cite the duplicate by phone. (...).

~

~

On the other hand, the lack of proactive responsibility was confirmed.

The concept of proactive responsibility is linked to the concept of compliance.

regulatory enforcement or compliance, already present in other regulatory areas (we refer to

We refer, for example, to the provision of article 31 bis of the Penal Code).

Thus, article 24 of the RGPD determines that “1. Considering the nature, the

scope, context and purposes of the treatment as well as the risks of different probabilities.

ity and seriousness for the rights and freedoms of natural persons, the person responsible

of the treatment will apply appropriate technical and organizational measures in order to guarantee

czar and be able to demonstrate that the treatment is in accordance with this Regulation. Gave-

These measures will be reviewed and updated as necessary.

2. When they are provided in relation to treatment activities, between

the measures mentioned in section 1 shall include the application, by the res-

responsible for the treatment, of the appropriate data protection policies”.

Proactive responsibility implies the implementation of a compliance model and

management of the RGPD that determines the generalized fulfillment of the obligations

in terms of data protection. It includes the establishment, maintenance, ac-

updating and control of data protection policies in an organization, especially

especially if it is a large company, -understood as the set of guidelines that governs

generate the performance of an organization, practices, procedures and tools-, dis-

of privacy by design and by default, which guarantee compliance with the

RGPD, that prevent the materialization of risks and that allows you to demonstrate your compliance.

filing.

Pivot on risk management. As established in Report 0064/2020

of the Legal Office of the AEPD shows the metamorphosis of a system that has

gone from being reactive to becoming proactive, since "at the present time,

It must be borne in mind that the RGPD has meant a paradigm shift when approaching

give the regulation of the right to the protection of personal data, which becomes the foundation

be based on the principle of "accountability" or "proactive responsibility" as

The AEPD has repeatedly pointed out (Report 17/2019, among many others) and it is re-

takes in the Statement of Reasons of the LOPDGDD: "the greatest novelty presented by the

Regulation (EU) 2016/679 is the evolution of a model based, fundamentally, on

in the control of compliance to another that rests on the principle of responsibility

active, which requires a prior assessment by the person in charge or by the person in charge of the

treatment of the risk that could be generated by the treatment of personal data.

personnel to, based on said assessment, adopt the appropriate measures".

It requires a conscious, committed, active and diligent attitude. consciousness

assumes knowledge of your organization by the data controller and

of how it is affected by data protection and the risks inherent to the

personal data processing; Commitment involves the will to comply and the

be truly responsible for the implementation of protection policies

of data in the organization; the active attitude is related to proactivity,

effectiveness, efficiency and operability; and diligence is the care, zeal and dedication

tion put into compliance.

Based on the foregoing, it can be affirmed that, from the instruction of the procedure, as

as inferred from the proven facts and considering the context of article 24 of the

RGPD in relation to VDF, it was verified, among others, the lack of an effective model of

avoidance of the risk of identity theft, the absence of security measures
adequate and tending to ensure the procedure of identification and delivery of
the SIM card, the materialization of the risks, the delayed temporary reaction to the
events described, in addition to the insufficiency of the measures adopted (because it has reacted
mentioned when receiving the requirements of the AEPD and has not avoided the subsequent repetition
as shown by the three subsequent claims filed with the AEPD).

Also, despite having a document called "security policy", it
does not imply the implementation of an effective model to avoid the risk of impersonation
identity, nor the implementation of a review, reinforcement, improvement and con-
control of the security measures applied in the different channels aimed at ensuring
rar the procedure of identification and delivery of the SIM card, in order to avoid the
materialization of fraud.

Especially when the SIM card constitutes the physical support through which access to
the personal data of the affected person. If its availability is not guaranteed
tion and control, access to the personal data of the owner, as well as the possible use or uses
by third parties, it becomes a threat that can have devastating effects
in the lives of these people.

On the other hand, according to the principle of proactive responsibility itself, it is the responsibility
responsible for the treatment that must determine what are the security measures to be
to implement, since only the latter has in-depth knowledge of its organization, of its
the treatments carried out, the risks associated with them and the me-
precise security measures to be implemented to make the principle of integrity effective.
ity and confidentiality.

However, it has been proven that the measures implemented by VDF are insufficient.
and not only because it has been overcome and the transfer of personal data
to a third party.

In a non-exhaustive manner and by way of example, we will look at (...).

Thus, from the documentation sent by VDF, the lack of specific instructions is inferred.

questions about what specific data should be requested from the caller to make a change

of SIM, referring to some additional rules, such as: (...).

The personal data associated with the security policy are the basics of any

client: (…). It is enough to have basic data of a client to be able to overcome the policy.

security, without any additional questions being asked regarding any

data that only the operator and its client know. No additional requirement

river is required.

Likewise, VDF has not provided any of the recordings of the calls made.

das for the change of SIM cards, alleging that the term of conservation of this

has expired. It is noteworthy that a total of XXX cases were detected by the operator

in which the security policy has been exceeded and being aware of the situation

at least in such cases the recordings or the transcript would have been preserved.

tion of these

Thus, the fraud known as "SIM Swapping" is a criminal technique

consisting of obtaining a duplicate of the SIM card associated with a telephone line

ownership of a user, in order to impersonate their identity to obtain access

so to your social networks, instant messaging applications, banking applications,

you laugh or electronic commerce, in order to interact and carry out operations in your

name, authenticating by means of a username and password previously taken from

that user, as well as with the double factor authentication when receiving the confirmation SMS.

mation in their own mobile terminal where they will have inserted the duplicate SIM card.

It should be noted that in the first phase of this type of scam the impersonator considers

fraudulently mislead login details or online banking credentials

of the client, but he needs to be able to know the verification code, second factor of increase

authentication, to be able to execute any operation. The moment you achieve

the duplicate SIM card already also has access to this second authentication factor.

tion and, therefore, from that moment you can carry out the acts of patrimonial disposition

nial you want.

Therefore, it is the responsibility of the operator to establish adequate requirements

effective and efficient that, although a quick reading may seem very strict,

a much more careful reading has shown that they were not. Whereupon, the

scam or impersonation, which apparently could seem complex and difficult, it is seen that

it has not been so due to the inadequacy of the security measures at the time of

ensure that it is the owner of the SIM card or the person authorized by him who requests

the duplicate.

All this, what it denotes is a lack of diligence in risk management, as well as

a reactive and not proactive attitude focused from the design and the inability to determine

show compliance.

FOURTH: Treatment of personal data and data controller

Article 4 of the RGPD, under the heading "Definitions", provides the following:

“1) «personal data»: all information about an identified or identifiable natural person.

reliable (“the interested party”); An identifiable natural person shall be deemed to be any person whose

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

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

identification, an online identifier or one or more elements of the physical identity

ca, physiological, genetic, psychic, economic, cultural or social of said person;

2) «processing»: any operation or set of operations carried out on data

personal data or sets of personal data, either by automated procedures

ized or not, such as the collection, registration, organization, structuring, conservation,

adaptation or modification, extraction, consultation, use, communication by transmission

sion, dissemination or any other form of authorization of access, collation or interconnection,

limitation, suppression or destruction".

7) "responsible for the treatment" or "responsible": the natural or legal person, authori-

public entity, service or other body that, alone or jointly with others, determines the purposes and

means of treatment; if the law of the Union or of the Member States determines

determines the purposes and means of the treatment, the person responsible for the treatment or the criteria

specific for their appointment may be established by the Law of the Union or of the

Member states".

VODAFONE ESPAÑA, S.A.U. is responsible for data processing referred to

two in the exposed antecedents, since according to the definition of the article

4.7 of the RGPD is the one that determines the purpose and means of the treatments carried out

with the purposes indicated in its Privacy Policy and that are detailed in the

guys tested.

Likewise, the issuance of a duplicate SIM card supposes the treatment of the damages

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

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

by an identifier (article 4.1) of the RGPD).

In this sense, it should be clarified that, inside the mobile terminal, the card is inserted
SIM. It is a smart card, in physical format and of reduced dimensions, which contains
It has a chip in which the service key of the subscriber or subscriber is stored.
gives to identify itself to the network, that is, the customer's mobile phone number
MSISDN (Mobile Station Integrated Sergvices Digital Network - Mobile Station of the
Integrated Services Digital Network-), as well as the personal identification number
of the subscriber IMSI (International Mobile Subscriber Identity - International Identity of the
mobile subscriber-) but can also provide other types of data such as information
tion on the telephone list or the calls and messages list.

The SIM card can be inserted into more than one mobile terminal, provided that it is
is released or is from the same company.

In Spain, since 2007, through the Unique Additional Provision of the Law
25/2007, of October 18, on the conservation of data related to communications
electronic networks and public communications networks, it is required that the holders of all
All SIM cards, whether prepaid or contract, are duly identified.
two and registered. This is important because subscriber identification will be important.
dispensable to register the SIM card, which will mean that when obtaining
a duplicate of this the person who requests it must also identify himself and that
your identity coincides with that of the owner.

In short, both the personal data (name, surnames and DNI) that are processed to issue
Get a duplicate SIM card as your own SIM (Subscriber Identity Module) card
that uniquely and unequivocally identifies the subscriber in the network, are character data
personal data, and its treatment must be subject to data protection regulations.
cough.

FIFTH: Allegations adduced to the Resolution Proposal.

We proceed to respond to them according to the order set out by VDF (the operation

Dora also refers in its entirety to the allegations presented on the 3rd of

March 2021):

PREVIOUS: ABOUT WHAT CONSTITUTES THE PURPOSE OF THE SANCTION PROCEDURE

TIONER.

As a previous allegation, VDF points out that the Resolution Proposal proposes the

imposition of a fine of 4,000,000'00 for an alleged infringement of articles

5.1.f) and 5.2 of the RGPD, infraction classified as very serious in article 83.5.a) of the

RGPD and by article 72.1 of the LOPDGDD, because VDF would have violated the

principles of integrity and confidentiality and proactive responsibility, by facilitating

SIM card duplicates to people who are not the holders of the mobile lines,

after the overcoming by these third parties of the security policies implemented by

VDF.

Likewise, it states that the sanctioning file has its origin in nine

claims filed with the Agency, although it has not only taken into account

the concrete facts and specificities that occurred in those cases, but it has

prosecuted the security measures adopted by VDF in general.

Indeed, and as has been shown throughout the procedure

sanctioning, the AEPD after various sanctioning procedures for identity fraud

entity filed with VDF, and as a result of 9 more claims for identity fraud, which

implied on the part of the data controller the issuance of a duplicate of the card

customer's SIM card (after which there have been serious economic damages to the

affected) investigates in depth the origin of the problem in order to find out if

day be due to punctual errors -as VDF claimed in many cases- or it was due to

a flaw in the privacy protection model.

The focus is not on the third parties that have exceeded the security policies, but

in why they have overcome them; that is, the condition, characteristics and

adequacy of the policies cited to the data protection regulations and the current

information from the data controller in this regard.

We must mean that, therefore, in this case the AEPD has focused not so much on

the lack of legitimacy in the processing of personal data but in the policy of pro-

entity data protection.

FIRST. LIMITATION OF THE OBJECT OF THE PROCEDURE TO THE EXAMINATION OF THE

TECHNICAL AND ORGANIZATIONAL MEASURES.

VDF indicates that the purpose of this procedure should be limited to determining whether

adopted the appropriate technical and organizational measures to avoid, to the extent

Wherever possible, duplicate SIM cards are issued to parties other than the owners.

lares of mobile lines. Prosecution cannot be extended to actions

earlier and later carried out by cybercriminals.

The Agency is surprised by the fact that it claims that we have not delimited the operations

tions or treatment activities when the Fourth Law Basis of the

Motion for a Resolution states that "the purpose of this file is not (...), but the

effective defense of the fundamental right to data protection for data processing

carried out by VDF" without at any time extending its "prosecution to the actions

previous and subsequent situations carried out by cybercriminals"; circums-

focusing on analyzing the procedures followed to manage requests for

change of SIM by VDF, not by other entities, such as financial ones, which

voca.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

The SIM card identifies a phone number and this number, in turn, identifies your
headline. In this sense, the Judgment of the CJEU in case C -101/2001 (Lindqvist) of
6.11.2003, section 24, Rec. 2003 p. I-12971: “The concept of "personal data" that
uses Article 3(1) of Directive 95/46 includes, in accordance with the
definition that appears in article 2, letter a), of said Directive "all information on
an identified or identifiable natural person". This concept includes, without a doubt, the
name of a person together with their telephone number or other information regarding
their working conditions or their hobbies”.

Also, this opinion is singled out in relation to mobile telephony devices
that allow the location of the interested party, in Opinion 13/2011 on services
of geolocation in smart mobile devices (document WP185):

“Smart mobile devices. Smart mobile devices are
are inextricably linked to natural persons. Normally there is
direct and indirect identification. First of all, the operators of
telecommunications that provide access to the mobile Internet and through
GSM network normally have a record with the name, address and
the bank details of each customer, together with several unique numbers of the
device, such as IMEI and IMSI. (…)”

In short, the questioned treatment activity has been the specific procedure
co for the change of VDF SIM card and the adequacy of security measures

implemented by VDF within the framework of risk management for the correct identification

tion of customers at the time of issuing the duplicate SIM card.

SECOND. COMPLIANCE WITH THE PRINCIPLE OF CONFIDENTIALITY AND IN-

INTEGRITY (SAFETY GUARANTEES) AND RESPONSIBILITY

PROACTIVE DAD.

VDF argues that it has complied with the principles of confidentiality and integrity

and proactive responsibility, as well as with the obligation to adopt the technical measures

adequate security measures and organisation: the security measures adopted by VDF do not have

They are not static, but rather they have been revised and updated over time.

over time.

Thus, it recounts again the actions carried out consisting of carrying out actions

of mitigation in the two VDF channels in which you can make changes of

SIM:

(...).

In this regard, it should be noted that it is precisely the fact that we find ourselves faced with fraud

of a third party makes it necessary to ensure that the person to whom the certificate is issued

duplicate SIM card is who it really claims to be and steps should be taken

adequate preventive measures to verify the identity of a person whose

data will be processed as recognized in the Legal Basis

co Seventh of the SAN, SCA, of May 5, 2021 (“On the other hand, regarding the fact

that we are facing the fraud of a third party, as we said in the SAN of 3

October 2013 (Rec. 54/2012) -: "Precisely for this reason, it is necessary to ensure

that the person who hires is who they really say they are and measures must be taken

adequate preventive measures to verify the identity of a person whose data

data are going to be processed...").

Throughout this proceeding, VDF has repeatedly stated that the du-

Fraudulent applications of the cards have occurred after having overcome the frauds

givers your security policy. Considers that it is inevitable that despite the existence

tenure of the security policy there may be cases in which through certain

mechanisms said security policy can be fraudulently surpassed

without there being any reproach to VDF.

However, it has been proven that VDF's security policy has been

insufficient for the adequate protection of the fundamental rights of people.

na whose SIM cards have been fraudulently duplicated; Taking into account that

the adoption of measures has occurred not after the analysis of the risks involved

the processing of data for the issuance of SIM card duplicates, carried out by

VDF, but when the facts have been made known to them, by transferring

of the claims filed with the AEPD; which reveals a con-

VDF's reactive conduct in the face of faits accomplis (communication of claims)

rather than the proactive conduct required by the GDPR that would require continuous analysis.

nated of the risks and the adoption of the corresponding measures to try to mi-

mitigate them, especially taking into account the economic damages that could be derived

of the subsequent use of duplicates of these fraudulent SIM cards, as has been

do demonstrated in the procedure.

In short, this allegation cannot be taken into consideration because VDF has not

complied with the obligation to reliably prove compliance with the principle

of proactive responsibility (article 5.2 of the RGPD) through continuous process" of

adaptation and "continuous management of the potential risks associated with the treatment of data", which has made it possible for VDF to issue fraudulent duplicates to third parties.

ros.

THIRD. THE ADOPTION OF TECHNICAL AND ORGANIZATIONAL MEASURES IS NOT AN ABSOLUTE OBLIGATION.

VDF alleges in its defense that the adoption of technical and organizational measures is not an absolute obligation: the figures in the file are a relevant indication that VDF has complied with the principle of integrity and confidentiality.

Thus, in support of this allegation, VDF indicates that the figures in the file demonstrate that VDF has complied with the principle of integrity and confidentiality; it is-crying out as arguments that VDF has proceeded to implement measures objectively suitable to protect the integrity and confidentiality of personal data.

personal data of the clients, taking into account the number of cases in which said measures security measures have been overcome, taking as a reference the temporary period poral in which the facts that are the subject of these proceedings are framed, that is, from July 29, 2019 (case of Claimant 5, folio 109 of the file) until June 2, 2020 (case of Claimant 8, folio 450 of the file), they indicate that VDF has rejected a total of X.XXX requests for duplicate SIM cards, avoiding potential fraud problems and XXX cases have materialized, which demonstrates It would appear that the implemented security measures work, according to VDF.

First of all, and about the fact that the adoption of technical and organizational measures is not an absolute obligation, which VDF alleges, it should be noted that no obligation is required. tion of result, but of activity, but to evaluate said activity and implement-measures and their consideration as "adequate" it is inevitable to analyze the methods two used by the third party to illicitly access the duplication process, the results safeguards implemented by VDF and inevitably, the result. Those three elements

These are the ones that are going to determine the adequacy to the risk and not how it intends to focus the

debate, VDF on whether or not their system is infallible.

The risk approach and the flexible risk model imposed by the RGPD -based on

of the double configuration of security as a principle relating to the treatment and

an obligation for the person in charge or the person in charge of the treatment - does not impose in any

In any case, the infallibility of the measures, but their constant adaptation to a risk,

that, as in the case examined is true, probable and not negligible, high and with

a very significant impact on the rights and freedoms of citizens.

Second, it should be noted that what these data make clear is that VDF is aware of

that of the total requests for duplication of SIM cards likely to be confirmed,

considered as fraudulent, which according to VDF's own criteria, would amount to X.X-

XX in the time period in which the actions of this procedure are framed.

taking into account the security measures implemented, XXX, that is, the

X,XX % of applications likely to be considered fraudulent are not detected

by VDF, and that VDF understands that this percentage assumes that the measures im-

planted are working satisfactorily.

Although in the opinion of the AEPD, security measures that allow a percentage in

around XX % of fraudulent duplicate SIM card issuance highlights the

insufficiency of these security measures adopted and the need for the

of VDF adequate measures are adopted to significantly reduce the cases of

fraudulent duplicate SIM cards.

In short, this allegation cannot succeed either, moreover, because it has been found that the percentage of cases in which the measures were exceeded of security adopted by VDF are close to XX% of the requests susceptible of being considered fraudulent are not detected through the application of the me- measures contained in the security policy that VDF claims to have implemented for this treatment.

QUARTER. LACK OF NEGLIGENCE IN THE ACTION OF VDF.

VDF affirms that its action has not been negligent. He argues in his defense that in the present sanctioning procedure, the circumstances of nine cases have been evaluated. you are concrete; that the figures in the file (which indicate that they have not been discussed by the Agency) show that we are dealing with isolated cases, of which that it can be inferred that VDF's action was not negligent; for all the me- measures adopted by VDF to prevent fraudulent duplication of cards; performs it- criminal activities of third parties to access certain personal data- those of those affected; and finally the existence of human errors that have led to the issuance of fraudulent duplicates.

It is not true, as VDF pretends to show that in this proceeding have evaluated the circumstances of nine specific cases, since, as has been As stated above, this procedure, starting from the nine claims, is has directed to analyze whether the technical and organizational measures adopted by VDF to the issuance of duplicate SIM cards to holders of telephone lines are appropriate to ensure the mitigation of possible risks to the rights and freedoms fundamental liberties of the holders of the lines.

The circumstances of the nine cases in which a claim has been filed with the AEPD reveal the insufficiency of the security measures adopted by VDF, which also recognizes that such measures have been insufficient in a total

of XXX cases in the period referred to in this sanctioning procedure, which

which shows that security measures do not fail only in isolated cases such as pre-

tends to assert VDF.

In addition, it must be taken into account that the seriousness of the proven facts that are

reflected in the social alarm generated by the realization of these fraudulent practices,

without determining the number of claims filed.

VDF refers, for its discharge, to the set of security measures that it has

adopted (a little before and during the sanctioning procedure) and

which says that it is renewed over time. On this particular meaning, in

firstly, that the security measures adopted by VDF have already initiated the procedure

sanctioning procedure do not affect the infraction already committed. Second, that the me-

measures implemented are the minimum required of any organization with the characteristics

characteristics and in the context in which a telecommunications operator operates. One re-

step to the same shows it. For example, the forwarding of communications addressed to

its workers and distributors warning about fraud and the specific measures of

implanted security forms part of an ordinary action of the person in charge of the

treatment (without this it is impossible for these to be effective); the same happens with the

SIM card blocking or message restriction once fraud is detected (not

would be acceptable to allow the continuation of the operation by the offender) and mark the

customer as a victim of fraud.

As has been proven, these security measures were neither adequate nor sufficient.

since the transfer of data to third parties has occurred without reliably verifying

the identity of the interested parties.

VDF mentions in its defense the actions of the criminals. The lack of me

security measures is an objective fact; such non-compliance is alien, moreover, to

the actions of the third parties to whom VDF has transferred the data, in the sense that the

criminal activity carried out by the latter does not influence the commission of the crime.

fraction. Quite the contrary, the lack of security measures is what makes possible the

criminal activity.

The fraudulent intervention of a third party, what has been revealed is the poor analysis

of the risks, as well as the insufficient implementation, review and control of the measures

security by the operator. Third parties other than the owners of the data

they have exceeded the security measures established by VDF on multiple occasions.

This shows us that the identification of the owner of the data did not occur with the

sufficient guarantees, regardless of whether the identification was made by the

holder himself or by a third party fraudulently.

VDF states that the duplicate SIM cards have occurred as a result of

human errors.

The human factor, the obvious possibility of making mistakes by human beings,

is one of the most important risks to always consider in relation to the determination

removal of security measures. The data controller must have

human error as a more than probable risk. Human errors are combated

from the risk approach, analysis, planning, implementation and control of the

adequate and sufficient technical and organizational measures.

This means that the significant number of human errors that are

produced in VDF continuously, constantly and repeatedly, as can be seen

of the proven facts.

Once, twice, it may be a human error that exceeds the measures

of security. Continuous human errors, what they externalize is a more pro-

rooted in the organization, a lack of vision of risks, analysis and planning

tion (privacy by design), an absence of dimensioning of the measures

of security, an omission in the implementation of the adequate ones or of revision of the

inadequate, the non-existence of demonstration of compliance… In short, a lack

of appropriate security measures and a breach of the obligations derived from

proactive responsibility, especially when the "errors" persist over time.

po (considering the subsequent claims filed with the AEPD against VDF

for similar acts after the initiation of the sanctioning procedure).

A criminal may attempt to cause human error, but it is security measures

adequate capacity who act as a brake. It is therefore palpable the lack of diligence of

VDF.

On the other hand, and strictly with regard to negligence in the actions of VDF, it is

point out that the SAN - Contentious-Administrative Chamber- 392/2015, of November 17

that in its Third Legal Foundation includes the doctrine of the Constitutional Court

on the application to sanctioning administrative law of the principles of order

penal, in the following terms:

“The Constitutional Court has repeatedly declared that the principles of the

penal code, among which is that of guilt, are applicable, with

certain nuances, to the sanctioning administrative law, since both are manifestations

punitive regulations of the State (STC 18/1987, 150/1991), and that

Strict liability or without

fault, by virtue of which the possibility of imposing sanctions for the mere

result, without proving a minimum of guilt even by way of mere negligence.

(SSTC 76/1990 and 164/2005).

The principle of culpability, guaranteed by article 25 of the Constitution, limits

the exercise of the "ius puniendi" of the State and requires, according to the Court

Constitutional in judgment 129/2003, of June 20, that the imposition of the

sanction is based on the requirement of the subjective element of guilt, to guarantee

emphasize the principle of responsibility and the right to a sanctioning procedure

with all the guarantees (STS of March 1, 2012, Rec 1298/2009).

Certainly, the principle of guilt, provided for in article 130.1 of the Law

30/1992, of November 26, on the Legal Regime of Public Administrations

cas and the Common Administrative Procedure, provides that they can only be

sanctioned for acts constituting an administrative infraction, those responsible

bles of the same, even by way of simple non-observance. Obviously, this knew

ne that said responsibility can only be demanded by way of intent or negligence,

being banished from the scope of sanctioning administrative law the so-called

called "strict responsibility", and understanding the guilty title the recklessness

negligence, negligence or inexcusable ignorance. This "simple non-compliance" cannot

be understood, therefore, as the admission in sanctioning administrative law

nator of strict liability, since the majority jurisprudence of our

Supreme Court (based on its rulings of January 24 and 25 and December 9,

May 1983) and the doctrine of the Constitutional Court (after its STC

76/1990), emphasize that the principle of guilt, even without express acknowledgment

implicit in the Constitution, is inferred from the principles of legality and prohibition of

excess (article 25.1 CE), or of the inherent requirements of a State

of Law, for which the existence of fraud or negligence is required (in this sense

STS of January 21, 2011, Rec 598/2008).

However, the mode of attribution of liability to legal persons

does not correspond to the forms of fraudulent or reckless guilt that

They are attributable to human behavior. Thus, in the case of violations

committed by legal persons, although the element of

guilt, it is necessarily applied differently from how it is done

with respect to natural persons. According to STC 246/1991 "(...) this construction

different from the imputability of the authorship of the infraction to the legal entity

It is born from the very nature of legal fiction to which these subjects respond.

The volitional element in the strict sense is lacking in them, but not the capacity to in-

violate the rules to which they are subject. Capacity of infraction and, by

therefore, direct blame that derives from the legal right protected by the norm

infringed and the need for such protection to be truly effective and

for the risk that, consequently, must be assumed by the legal entity that is

subject to compliance with said rule "(in this sense STS of November 24

of 2011, Rec 258/2009).

To the above must be added, following the judgment of January 23, 1998,

partially transcribed in the SSTS of October 9, 2009, Rec 5285/2005, and

of October 23, 2010, Rec 1067/2006, that "although the guilt of the

conduct must also be tested, must be considered in order to

assumption of the corresponding charge, which ordinarily the volitional elements

and cognitive skills necessary to appreciate it are part of the behavior

proven typical ta, and that its exclusion requires proving the absence of ta-

the elements, or in its normative aspect, that the diligence that

it was demandable by those who allege its non-existence; not enough, in short, to exonerate

tion in the face of typically unlawful behavior the invocation of authority

sense of guilt".

In the case that concerns us, the existence of illegality and culpability is notorious.

in the infringing conduct of the entity responsible for data processing

personal information, VDF, who, as the data controller for the emission of du-

SIM card applications, which decides on the purpose, content and use of the data

included in the treatment, has the obligation to act with greater diligence

ence when processing the issuance of duplicates, making sure to have the con-

sentiment of its owner, in order not to incur in the non-consensual treatment of their data.

personal cough. Said condition imposes a special duty of diligence when

carry out the use or treatment of personal data, in terms of compliance

performance of the duties that the legislation on data protection establishes for ga-

guarantee the fundamental rights and public freedoms of natural persons, and

especially his honor and personal and family intimacy, whose intensity is found

enhanced by the relevance of the legal rights protected by those rules and

the professionalism of those responsible or in charge, especially when they operate with

mo for profit in the data market; In this sense, the

SAN 392/2015, of November 17 (See its Third Law Basis).

In this regard, it is significant that the operator responsible for the treatment did not justify

duly verify the concurrence in his conduct of the diligence that was required of him

nor prove the adoption of the precautions required to avoid non-consensual treatment.

of the personal data that concerns us (the issuance of duplicate cards

SIM fraudulently), which must be attributed to the negligent conduct of VDF, with

regardless of whether the contracting took place before a distributor of said company.

company, or is carried out by telephone or telematics using by a third party the

personal data of the claimants passing the security measures to carry out

the duplication of SIM cards.

In conclusion, the purpose of this procedure has been aimed at analyzing whether the measures

techniques and organization adopted by VDF for the issuance of duplicate cards-

SIM cards to the holders of the telephone lines are appropriate to ensure the mitigation

tion of the possible risks to the fundamental rights and freedoms of the holders

lines, not to evaluate the circumstances that have occurred in nine cases.

specific objectives, taking into account the social alarm generated by the realization of

these fraudulent practices, without determining the number of claims

presented. Having been accredited the negligence due to the insufficiency of the me-

measures adopted, which has meant that at least XXX cases have been affected

gun recognizes VDF.

FIFTH. APPLICATION OF THE PRINCIPLE OF PROPORTIONALITY.

VDF states that subsidiarily and in the event that it is understood that it can

of imposing a sanction, considers the same disproportionate when understanding that

proposes a sanction of approximately 444,000 euros for each case, having to re-

its amount may be reduced by the circumstances it expresses.

Regarding the alleged disproportionality of the proposed sanction, it is convenient to indicate

note that the RGPD expressly provides for the possibility of graduation, by anticipating

fines subject to modulation, in response to a series of circumstances

of each individual case effective, proportionate and dissuasive (article 83.1 and 2

RGPD), general conditions for the imposition of administrative fines that do

have been analyzed by this Agency, to which must be added the criteria of

graduation foreseen in the LOPDGDD, object of development in the Eighth FD.

Furthermore, when demonstrating the proportionality of the sanction pro-

It should be noted that if the sanctions provided for in the previous regulations were applied,

above, taking into account that the infractions committed by VDF are classified as

very serious infractions and article 45.3 of the LOPD of 1999 provided that “The infractions

very serious violations will be sanctioned with a fine of between 300,001 and 600,000 euros.

for very serious infractions” for each of the claims, such as 9 re-

claims the fine that would have been imposed with the previous regulations would be

between 2,700,000 and 5,400,000 euros, with which the fine currently

The rate set would be within the range of the sanction provided for in the previous regulations, which

is no longer applicable.

Although it must be reiterated that the sanction is not imposed for those cases in which

claims have been filed, but because these cases highlight the non-compliance

security guarantees (article 5.1.f) RGPD) and responsibility

proactive liability (article 5.2 of the RGPD) that reveals the deficiency of

the security measures adopted by VDF in the processing of duplicate data

of SIM cards that allows the duplication of said SIM cards for fraudulent reasons.

cough.

In addition, it must be taken into account that the RGPD does not currently set a minimum amount.

and that article 83.5 establishes that “The infractions of the following dispositions

The following will be sanctioned, in accordance with section 2, with administrative fines of

EUR 20,000,000 maximum or, in the case of a company, an equivalent amount.

to a maximum of 4% of the total global annual turnover of the fiscal year

previous financial statement, opting for the highest amount”.

It should be noted that the agreed administrative fine will be effective because it will lead

the operator to comply with the proactive responsibility and to apply the technical measures

and organizational characteristics that guarantee a degree of security corresponding to the value of

treatment criticality. It is also proportional to the violation identified, in

particular to its severity, the circle of natural persons affected and the risks in the

that have been incurred and the financial situation of the company.

And finally, it is dissuasive. A dissuasive fine is one that has a dissuasive effect.

sory genuine. In this regard, the Judgment of the CJEU, of June 13, 2013, Ver-

salis Spa v Commission, C-511/11, ECLI:EU:C:2013:386, says:

“ 94.Regarding, first of all, the reference to the Showa judgment

Denko v Commission, cited above, it should be noted that Versalis interprets it

incorrectly. In fact, the Court of Justice, when pointing out in the paragraph

do 23 of said sentence that the dissuasive factor is valued taking into account

consideration a multitude of elements and not just the particular situation

of the company in question, he was referring to points 53 to 55 of the

conclusions presented in that matter by Advocate General Geelhoed,

he had pointed out, in essence, that the multiplier coefficient of characters
dissuasive ter may have as its object not only a "general deterrence", but
defined as an action to discourage all companies, in general,
that they commit the offense in question, but also a «deterrent»
specific action', consisting of dissuading the specific defendant from
don't break the rules again in the future. Therefore, the Court of
Justice only confirmed, in that sentence, that the Commission was not obligated
bound to limit its assessment to factors related solely to the following
particular situation of the company in question."

"102. According to settled jurisprudence, the objective of the multiplier factor
suasory and the consideration, in this context, of the size and the re-
global courses of the company in question lies in the desired impact
on the aforementioned company, since the sanction should not be insignificant, it is
especially in relation to the financial capacity of the company (in
this sense, see, in particular, the judgment of June 17, 2010,
Lafarge v Commission, C-413/08 P, ECR p. I-5361, section 104, and the car of 7
February 2012, Total and Elf Aquitaine v Commission, C-421/11 P, para.
82)."

The Judgment dated May 11, 2006 issued in the cassation appeal
7133/2003 establishes that: "It must also be taken into account that one of the criteria
governing the application of said principle administrative sanctioning regime (criterion
collected under the rubric of «principle of proportionality» in section 2 of article
131 of the aforementioned Law 30/1992) is that the imposition of pecuniary sanctions does not
must suppose that the commission of the typified infractions is more beneficial
for the offender than compliance with the rules violated".

Also important is the jurisprudence resulting from the Judgment of the Third Chamber

of the Supreme Court, issued on May 27, 2003 (rec. 3725/1999) that

says: Proportionality, pertaining specifically to the scope of the sanction,

constitutes one of the principles that govern the sanctioning Administrative Law, and

represents an instrument of control of the exercise of the sanctioning power by the

Administration within, even, the margins that, in principle, the standard indicates

applicable for such exercise. It certainly supposes a concept that is difficult to determine

a priori, but which tends to adapt the sanction, by establishing its specific graduation

within the indicated possible margins, to the seriousness of the constitutive act of the

infraction, both in its aspect of unlawfulness and culpability, weighing

as a whole the objective and subjective circumstances that make up the budget

de facto punishable -and, in particular, as it results from article 131.3 LRJ and PAC, the

intentionality or repetition, the nature of the damage caused and the recurrence

Inc-. (SSTS July 19, 1996, February 2, 1998 and December 20, 1999, en-

three many others).

SIXTH. NEW EVIDENCE PROVIDED BY VDF.

Finally, VDF lists the new tests that it intends to use in the present

sanctioning procedure for the purpose of proving their lack of guilt or the reduction

ja of the amount of the sanction. Namely, (…).

In this regard, it should be noted that article 89.2 of Law 39/2015, of October 1,

of Common Administrative Procedure establishes that “In the case of procedures

of a punitive nature, once the investigation of the procedure has concluded, the

instructor will formulate a resolution proposal that must be notified to the interested parties.

resados. The proposed resolution must indicate the disclosure of the process

proceeding and the term to formulate allegations and present the documents and information

tions that are deemed pertinent", so the documents provided in this allegation

tion are understood to be pertinently provided and are incorporated into the applicant's file.

feel procedure.

Although VDF's assessment is not shared that they should be considered as

supporting documents of his lack of guilt in this file, or, in

its case, modulate downwards the sanction proposed by the Agency, since the documents

The documents provided do not provide additional information to that contained in the Documents.

Documents 4 and 7 proposed as evidence to practice in the Brief of Allegations to the

Start Agreement:

(...).

In accordance with the foregoing, we must conclude that, after analyzing the

pleadings to the initial Agreement as well as to the Resolution Proposal, the

facts and legal foundations on which they are based, do not distort the Facts or the

Grounds of Law included both in the Initial Agreement and in the Proposal.

ta of resolution or in this Resolution.

SIXTH: Principles relating to treatment.

Considering the right to the protection of personal data as the right

natural persons to have their own data, it is necessary to determine the

principles that make it up.

In this sense, article 5 RGPD, referring to the "Principles related to treatment"

has:

1. The personal data will be:

a) processed in a lawful, loyal and transparent manner in relation to the interested party ("lawful

trust, loyalty and transparency»);

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

68/88

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

riorly in a manner incompatible with said purposes; (...);

c) adequate, pertinent and limited to what is necessary in relation to the purposes for

those that are processed ("data minimization");

d) accurate and, if necessary, updated; All reasonable steps will be taken

entitled to delete or rectify without delay the personal data that

are inaccurate with respect to the purposes for which they are processed (“accuracy”);

e) maintained in a way that allows the identification of the interested parties during

no longer than is necessary for the purposes of processing the personal data;

(…)

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

including protection against unauthorized or unlawful processing and

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

appropriate technical or organizational measures ("integrity and confidentiality").

2. The controller will be responsible for compliance with the provisions

in paragraph 1 and able to demonstrate it ("proactive responsibility").

The principle of data security requires the application of technical or organizational measures.

appropriate organizational measures in the processing of personal data to protect said

data against access, use, modification, dissemination, loss, destruction or accidental damage

dental, unauthorized or illegal. In this sense, security measures are key to

when guaranteeing the fundamental right to data protection. It is not possible the
existence of the fundamental right to data protection if it is not possible to guarantee
the confidentiality, integrity and availability of our data.
In this sense, recital 75 of the RGPD determines: The risks to the rights
rights and freedoms of natural persons, of varying gravity and probability, can
are due to the processing of data that could cause physical damage,
material or immaterial, in particular in cases where the processing may
give rise to problems of discrimination, identity theft or fraud, fi-
financial losses, reputational damage, loss of confidentiality of data subject to secre-
professional creed, unauthorized reversal of pseudonymization, or any other per-
significant economic or social judgement; in the cases in which the interested parties are deprived
two of their rights and freedoms or are prevented from exercising control over their data
personal; in cases in which the personal data processed reveal the origin
ethnic or racial, political opinions, religion or philosophical beliefs, militancy
in trade unions and the processing of genetic data, data related to health or social data.
sexual life, or criminal convictions and infractions or security measures such as
nexus; in cases in which personal aspects are evaluated, in particular the analysis
analysis or prediction of aspects related to performance at work, economic situation,
mica, health, personal preferences or interests, reliability or behavior, situation
tion or movements, in order to create or use personal profiles; in cases where
those that process personal data of vulnerable people, in particular children; or in
cases in which the treatment involves a large amount of personal data and
affects a large number of stakeholders.
Likewise, recital 83 of the RGPD establishes: In order to maintain the security and
avoid that the treatment violates the provisions of this Regulation, the controller
responsible or the person in charge must evaluate the risks inherent to the treatment and apply mea-

given to mitigate them, such as encryption. These measures must guarantee a level of security

adequate security, including confidentiality, taking into account the state of the tech-

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

personal to be protected. When assessing the risk in relation to the safety of

the data, the risks that derive from the treatment of the data must be taken into account.

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

personal data transmitted, stored or otherwise processed, or the communication

or unauthorized access to said data, which is particularly likely to cause damage

and physical, material or immaterial damages.

We must attend to the unique circumstances of the nine claims presented.

ted, through which it can be verified that, from the moment in which the

impersonating person performs the replacement of the SIM, the victim's phone stays

gives no service, passing control of the line to the impersonators. In consequence

Consequently, the claimants see their powers of disposal and control over their

personal data, which constitute part of the content of the fundamental right to

data protection as indicated by the Constitutional Court in the Judgment

292/2000, of November 30, 2000 (FJ 7). So, by getting a duplicate

tion of the SIM card, it is possible under certain circumstances, the access to the

contacts or to the applications and services that have as a recovery procedure

password generation the sending of an SMS with a code to be able to modify the passwords

yes. In short, they may supplant the identity of those affected, being able to access and

control, for example: email accounts; bank accounts; application-

nes like WhatsApp; social networks, such as Facebook or Twitter, and much more. In re-

sinking accounts, once the access code has been modified by the supplanted-

users lose control of their accounts, applications and services, which is a great

threat.

Hence, the security and confidentiality of personal data are considered

essential to prevent data subjects from suffering negative effects.

In line with these provisions, recital 39 RGPD provides: All treatment

The processing of personal data must be lawful and fair. For natural persons you must-

make it absolutely clear that they are being collected, used, consulted or attempted to

otherwise personal data concerning them, as well as the extent to which said

data is or will be processed. The principle of transparency requires that all information and

communication regarding the processing of said data is easily accessible and easy

to understand, and that simple and clear language is used. This principle refers to

particular to the information of the interested parties on the identity of the person in charge of the

treatment and the purposes of the same and to the information added to guarantee a treatment

fair and transparent treatment with respect to the natural persons affected and their right

right to obtain confirmation and communication of personal data concerning them.

nan that are subject to treatment.

Natural persons must be aware of the risks, standards, safeguards,

guards and the rights related to the processing of personal data as well as the

way to enforce your rights in relation to the treatment. In particular, the fi-

specific terms of the processing of personal data must be explicit and legitimate.

mos, and must be determined at the time of collection. The personal data of

must be adequate, relevant and limited to what is necessary for the purposes for which

be treated. This requires, in particular, ensuring that it is limited to a strict minimum

its retention period. Personal data should only be processed if the purpose of the processing
treatment could not reasonably be achieved by other means. To ensure that

personal data is not kept longer than necessary, the person responsible for the
treatment must establish deadlines for its suppression or periodic review. They must to-
take all reasonable steps to ensure that they are rectified or deleted
personal data that is inaccurate. Personal data must be treated in a
way that guarantees adequate security and confidentiality of the personal data
purposes, including to prevent unauthorized access or use of such data and the
equipment used in treatment.
In short, it is the data controller who has the obligation to integrate the
necessary guarantees in the treatment, with the purpose of, under the principle of
proactive responsibility, comply and be able to demonstrate compliance, at the same
while respecting the fundamental right to data protection.
Recital 7 provides: (...) Individuals must have control of their
own personal data. (…)
The facts declared previously proven, are constitutive of a violation
of article 5.1.f) of the RGPD by providing duplicate VDFs of the SIM card to third parties.
people who are not the legitimate owners of the mobile lines and even modify the ownership
larity of the contracted services, after overcoming by the supplanting people
of the security policies implemented by the operator, which shows a breach
Compliance with the duty to protect customer information.

This unauthorized access to the SIM card is decisive for the actions

developed by the supplanting people whose purpose is to obtain

have an economic benefit, since the impersonator takes advantage of the space of time

that elapses until the user detects the fault on the line, contacts

with the operator, and this detects the problem, to carry out fraudulent banking operations.

dulent after accessing the online banking passwords of the legitimate subscriber.

The issuance and delivery of the duplicate to an unauthorized third party implies for those affected

two the loss of control of your personal data. Therefore, the value of that data

personal, integrated in a physical support -SIM card-, is real and unquestionable, reason

for which VDF have a legal duty to ensure your safety, just as it would with

any other assets.

It is worth mentioning ruling 292/2000, of November 30, of the Constitutional Court

tutional, which configures the right to data protection as an autonomous right

and independent that consists of a power of disposition and control over the data

personal data that empowers the person to decide which of these data to provide

to a third party, be it the State or an individual, or what data this third party may collect, and

which also allows the individual to know who owns that personal data and for what,

being able to oppose that possession or use. Thus, in accordance with the legal foundations

cos 4, 5, 6 and 7 of the judgment of the high court:

"4. Without needing to explain in detail the wide possibilities that information

matic offers both to collect and to communicate personal data or the

undoubted risks that this can entail, given that a person can ignore

rar not only what are the data that concern you that are collected in

a file but also if they have been transferred to another and for what purpose, it is

enough to indicate both extremes to understand that the fundamental right

to privacy (art. 18.1 CE) does not provide sufficient protection by itself

in the face of this new reality derived from technological progress.

However, with the inclusion of the current art. 18.4 CE the constituent put of

highlighted that he was aware of the risks that the use of the information could entail.

and entrusted to the legislator the guarantee of both certain fundamental rights

mental and the full exercise of the rights of the person. That is, in-

incorporating a guarantee institute "as a form of response to a new formation

a concrete threat to the dignity and rights of the person", but

which is also, "in itself,

a fundamental right or freedom

(STC 254/1993, of July 20, FJ 6). Concern and purpose of the constituent

which is evident, on the one hand, if one takes into account that from the draft

The constitutional text already included a section similar to the current art. 18.4 EC

and that this was later expanded by accepting an amendment to include-

ra its final paragraph. And more clearly, on the other hand, because if in the debate in the

Senate, some doubts were raised about the need for this section of the

precept given the recognition of the rights to privacy and honor in the

initial section, however, were dissipated by highlighting that these

rights, in view of their content, did not offer sufficient guarantees against

the threats that the use of information technology could entail for the protection of

private life. So the constituent wanted to guarantee through the

current art. 18.4 EC not only a specific scope of protection but also

more suitable than the one that fundamental rights could offer, by themselves.

such mentioned in section 1 of the precept.

5. (…)

Well, in these decisions the Court has already declared that art. 18.4 EC

contains, under the terms of the STC 254/1993, a guarantee institute for the

rights to privacy and honor and the full enjoyment of the other rights

of citizens which, furthermore, is in itself "a fundamental right or freedom

mental health, the right to liberty in the face of potential attacks on the dignity

and the freedom of the person from an illegitimate use of the treatment

mechanized data, what the Constitution calls 'informatics'", which has been

called "computer freedom" (FJ 6, later reiterated in the

SSTC 143/1994, FJ 7, 11/1998, FJ 4, 94/1998, FJ 6, 202/1999, FJ 2). The guarantee-

privacy of a person's private life and reputation today have a dimension

positive pressure that exceeds the scope of the fundamental right to intimidation.

ity (art. 18.1 CE), and that translates into a right of control over the data

relating to the person himself. The so-called "computer freedom" is thus the right to

control the use of the same data inserted in a computer program (ha-

beas data) and includes, among other aspects, the citizen's opposition to

that certain personal data are used for purposes other than

the legitimate one that justified its obtaining (SSTC 11/1998, FJ 5, 94/1998, FJ 4).

This fundamental right to data protection, unlike the right to

privacy of art. 18.1 CE, with whom it shares the goal of offering efficient

effective constitutional protection of private personal and family life, attributes to

holder a bundle of powers consisting for the most part of the legal power

dictate of imposing on third parties the performance or omission of certain behaviors

ments whose specific regulation must be established by the Law, the one that conforms

to art. 18.4 CE must limit the use of information technology, either by developing the right

fundamental right to data protection (art. 81.1 CE), either regulating its exercise

cycle (art. 53.1 CE). The peculiarity of this fundamental right to protection

tion of data regarding that fundamental right as related as that of

intimacy lies, then, in its different function, which therefore entails

that also its object and content differ.

6. The function of the fundamental right to privacy of art. 18.1 CE is that of

protect against any invasion that may be carried out in that area of the

personal and family life that the person wishes to exclude from the knowledge of others and

of the interference of third parties against their will (for all

STC 144/1999, of July 22, FJ 8). Instead, the fundamental right to

data protection seeks to guarantee that person a power of control over

about your personal data, about its use and destination, with the purpose of preventing

its illicit and harmful traffic for the dignity and rights of the affected. Finally, the right

The right to privacy allows certain data of a person to be excluded from knowledge.

third party, for this reason, and this Court has said so (SSTC 134/1999, of 15

July, FJ 5; 144/1999, FJ 8; 98/2000, of April 10, FJ 5; 115/2000, of 10 of

May, FJ 4), that is, the power to protect your private life from publicity

No, darling. The right to data protection guarantees individuals a

power of disposal over such data. This guarantee imposes on the public powers

public authorities prohibiting them from becoming sources of such information without the

due guarantees; and also the duty to prevent the risks that may derive
avoid improper access or disclosure of such information. But that power
of disposition on the personal data itself nothing is worth if the affected
knows what data is held by third parties, who owns it, and
to what end
Hence the singularity of the right to data protection, since, on the one hand,
Its object is broader than that of the right to privacy, since the right
fundamental to data protection extends its guarantee not only to privacy
in its dimension constitutionally protected by art. 18.1 EC, but to
which this Court has on occasion defined in broader terms as
sphere of the assets of the personality that belong to the sphere of private life.
da, inextricably linked to respect for personal dignity (STC 170/1987,
of October 30, FJ 4), such as the right to honor, expressly cited in the
art. 18.4 CE, and likewise, in a very broad expression of art. 18.4 CE, al
full exercise of personal rights. The fundamental right to
Data protection extends the constitutional guarantee to those data that
are relevant to or have an impact on the exercise of any rights
rights of the person, whether or not they are constitutional rights and whether or not they are relative
honor, ideology, personal and family intimacy to any other cons-
formally protected.
In this way, the object of protection of the fundamental right to protection
of data is not reduced only to the intimate data of the person, but to any
type of personal data, whether intimate or not, whose knowledge or use by third parties
ros may affect their rights, whether fundamental or not, because their purpose
it is not only individual intimacy, for this is the protection that art.
18.1 CE grants, but personal data. Therefore, also

reaches those public personal data, which by the fact of being, of being

accessible to the knowledge of anyone, they do not escape the power of disposition

of the affected party because this is guaranteed by their right to data protection. Tam-

Also for this reason, the fact that the data is of a personal nature does not mean that it only

those related to the private or intimate life of the person have protection, but

that the protected data are all those that identify or allow the

identification of the person, being able to serve for the preparation of their profile

ideological, racial, sexual, economic or of any other nature, or that serve

for any other use that in certain circumstances constitutes a

threat to the individual.

But the fundamental right to data protection also has a se-

second peculiarity that distinguishes it from others, such as the right to privacy

personal and family of art. 18.1 EC. This peculiarity lies in its content,

since unlike the latter, which confers on the person the legal power

to impose on third parties the duty to refrain from any interference in the

privacy of the person and the prohibition of making use of what is thus known

(SSTC 73/1982, of December 2, FJ 5; 110/1984, of November 26, FJ

3; 89/1987, of June 3, FJ 3; 231/1988, of December 2, FJ 3; 197/1991,

of October 17, FJ 3, and in general the SSTC 134/1999, of June 15,

lio, 144/1999, of July 22, and 115/2000, of May 10), the right to pro-

data protection attributes to its holder a bundle of faculties consisting of different

those legal powers whose exercise imposes legal duties on third parties, which
are not contained in the fundamental right to privacy, and that serve the
essential function performed by this fundamental right: to guarantee the person
a power of control over your personal data, which is only possible and effective
vo imposing on third parties the aforementioned duties to do. Namely: the right
I agree that prior consent is required for the collection and use of the
personal data, the right to know and be informed about the destination and use of
that data and the right to access, rectify and cancel said data. In defi-
tive, the power of disposal over personal data (STC 254/1993, FJ 7).
7. From all that has been said, it follows that the content of the fundamental right to
Data protection consists of a power of disposition and control over data.
personal data that empowers the person to decide which of these personal data
provide to a third party, be it the State or an individual, or what this third party can
ro collect, and that also allows the individual to know who owns that data
and for what, being able to oppose that possession or use. These can-
disposition and control over personal data, which constitute part
of the content of the fundamental right to data protection are specified
legally empowered to consent to the collection, obtaining and access to
personal data, their subsequent storage and treatment, as well as their
possible use or uses, by a third party, be it the State or an individual. And that right-
right to consent to the knowledge and treatment, computerized or not, of the data
personal, requires as essential complements, on the one hand, the faculty
the right to know at all times who has these personal data and to what
use is subduing them, and, on the other hand, the power to oppose that possession and
applications.
Finally, they are characteristic elements of the constitutional definition of the right

fundamental to the protection of personal data the rights of the affected to

consent to the collection and use of your personal data and to know of the same

mos. And it is essential to make this content effective the recognition

protection of the right to be informed of who owns your personal data and with

what purpose, and the right to be able to oppose that possession and use by requiring

who corresponds to put an end to the possession and use of the data. Namely,

requiring the owner of the file to inform him of what data he has about his personal

person, accessing their appropriate records and seats, and what fate they have had-

do, which also reaches potential assignees; and, where appropriate, require

to rectify or cancel them.” (the underlining of all the paragraphs is

our)

Therefore, any action that involves depriving the person of those faculties

disposition and control over your personal data, constitutes an attack and a vulnerability

ration of their fundamental right to data protection.

There has also been a violation of the principle of proactive responsibility.

Directly related to the principle of proactive responsibility foreseen in the

article 5.2. of the RGPD is the “Responsibility of the data controller”

lie”, article 24 of the RGPD:

1. Taking into account the nature, scope, context and purposes of the treatment-

as well as the risks of varying probability and severity for the rights and liberties

freedoms of natural persons, the data controller will apply technical measures

appropriate technical and organizational measures in order to guarantee and be able to demonstrate that the treatment

ment is in accordance with these Regulations. These measures will be reviewed and

will update when necessary.

2. When they are provided in relation to treatment activities, in-

The measures mentioned in section 1 shall include the application, by the

responsible for the treatment, of the appropriate data protection policies.

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

certification canism approved under article 42 may be used as

elements to demonstrate compliance with the obligations by the responsible

ble of the treatment

In line with these provisions, recital 74 of the RGPD provides: You must

be established the responsibility of the data controller for any

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

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

be able to demonstrate the conformity of the treatment activities with the present Regulation-

ment, including the effectiveness of the measures.

Likewise, related to the principle of proactive responsibility is the

principle of "Data protection by design and by default", contained in the article

25 of the GDPR:

1. Taking into account the state of the art, the cost of the application and the nature

nature, scope, context and purposes of the treatment, as well as the risks of different probabilities.

ity and seriousness that the treatment entails for the rights and freedoms of the per-

physical persons, the data controller will apply, both at the time of determining

nar the means of treatment as at the time of the treatment itself, measures

appropriate technical and organizational techniques, such as pseudonymization, designed to apply

effectively implement the principles of data protection, such as the minimization of

data, and integrate the necessary guarantees in the treatment, in order to comply with the requirements

of this Regulation and protect the rights of the interested parties.

2. The data controller will apply the technical and organizational measures

with a view to guaranteeing that, by default, they are only processed

the personal data that is necessary for each of the specific purposes of the

treatment. This obligation will apply to the amount of personal data collected, to

the extension of its treatment, its conservation period and its accessibility. Such

measures shall in particular ensure that, by default, personal data is not accessed.

accessible, without the intervention of the person, to an indeterminate number of individuals

sicas

3. An approved certification mechanism may be used in accordance with article

42 as an element that proves compliance with the obligations established in

sections 1 and 2 of this article.

In line with these provisions, recital 78 of the GDPR provides:

The protection of the rights and freedoms of natural persons with respect to the

processing of personal data requires the adoption of technical and organizational measures

appropriate in order to ensure compliance with the requirements of this Regulation.

glament. In order to be able to demonstrate compliance with this Regulation, the

data controller must adopt internal policies and apply measures that

comply in particular with the principles of data protection by design and by default.

fect. Said measures could consist, among others, of minimizing the treatment

of personal data, pseudonymize personal data as soon as possible, transfer
parity to the functions and the processing of personal data, allowing interested parties
responsible for supervising data processing and the data controller creating and me-
improve security elements. When developing, designing, selecting and using applications,
services and products that are based on the processing of personal data or that
process personal data to fulfill their function, producers of
products, services and applications that take into account the right to protection
tion of data when developing and designing these products, services and applications,
and to ensure, with due regard to the state of the art, that those responsible
managers and data processors are in a position to comply with their obligations
tions regarding data protection. The principles of data protection
by design and by default must also be considered in the context of the
public contracts.

Specifically, in light of the RGPD recital 78, the principle of data protection
from the design is the key to be followed by the data controller to demonstrate
ensure compliance with the GDPR, since “the data controller must adopt
implement internal policies and implement measures that comply in particular with the principles of pro-
data protection by design and by default”.

In fact, data security is not achieved with the right equipment alone.
(hardware and software), but also requires the existence of standards
adequate organizational internals.

Throughout this proceeding, it has been proven that the procedures
of issuing VDF SIM card duplicates require a correct analysis, planning,
fication, establishment, maintenance, updating and control, including the demonstration
enforcement (observance of the principle of proactive responsibility), es-
especially in relation to adequate and sufficient security measures, with the

In order to guarantee the security of the personal data of Ma-

effectively and in particular, its custody, to prevent unauthorized access to the data.

applications of the SIM cards and/or services of their holders.

SEVENTH: General conditions for the imposition of the administrative fine.

Article 83.2 of the RGPD provides that:

Administrative fines will be imposed, depending on the circumstances of each

individual case, in addition to or as a substitute for the measures contemplated in art.

Article 58, paragraph 2, letters a) to h) and j). When deciding to impose an administrative fine

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

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

nature, scope or purpose of the processing operation in question

as well as the number of interested parties affected and the level of damages and losses.

who have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor

to alleviate the damages suffered by the interested parties;

d) the degree of responsibility of the data controller or data processor.

taking into account the technical or organizational measures that have been applied

under articles 25 and 32;

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

I lie;

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

gave the infringement and mitigate the possible adverse effects of the infringement;

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

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

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

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 question in re-

relationship with the same matter, compliance with said measures;

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

certificates approved in accordance with article 42, and k) any other factor

aggravating or mitigating circumstance applicable to the circumstances of the case, such as the benefits

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

through the infringement.

For its part, article 76 “Sanctions and corrective measures” of the LOPDGDD provides

ne:

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

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

two in section 2 of the aforementioned article.

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

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 treatment of

personal information.

c) The profits obtained as a result of committing the offence.

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

violation.

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

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

The impact on the rights of minors.

F)

g) Have, when not mandatory, a data protection officer.

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

alternative conflict resolution mechanisms, in those cases in which

those that exist controversies between those and any interested party. (…)"

In accordance with the precepts transcribed for the purpose of setting the amount of the sanction

as responsible for the infringement typified in article 83.5.a) of the RGPD, it proceeds

graduate the fine that corresponds to impose with respect to both infractions, prior va-

explanation of the allegations adduced for the purposes of a correct application of the principle

principle of proportionality.

On the one hand, the following aggravating factors have been taken into account:

- Article 83.2.a) GDPR:

 Nature, severity and duration:

In relation to the nature of the personal data on which

has lost the provision (temporarily), in addition to the telephone line

nica, affect in the case of the complaining parties one and six, in addition

of running out of service, to the remittance of a duplicate invoice with

the personal data of the legitimate owner of the line and in the case of
claimant party eight, to the subscription of a Mobile Service contract,
Broadband, Fixed and TV for Private Clients that contained the data
bank notes of its legitimate owner. These facts confirm the nature
nature of the infraction as very serious since it entails a loss of
disposal and control over personal data.
In relation to the time period with respect to which the events occurred,
in the Motion for a Resolution the allegation regarding
that does not exceed the year. The investigative body recognized its error of
appreciation, without, on the other hand, considering its relevance. the du-
ration of the facts occurs since July 29, 2019 (case of the

complaining party five) until June 2, 2020 (case of the complaining party)
crying eight). However, subsequently, this Agency has registered
Do up to three more claims denouncing similar facts. On
these claims, in accordance with article 65.4 of the LO-
PDGDD, has been transferred to the Data Protection Delegate of
VDF, to proceed with its analysis and respond to this Agency.
cia within a month.
.- Claim A: (…). Facts according to statements of the par-
claimant: Duplicates of the SIM card have been provided in
dates 01/31/2020, 04/27/2020 and 06/08/2020 (twice)

to third parties, running out of line and using said

third parties of your line to carry out fraudulent operations in the

claimant's bank account (cash withdrawal, request

loans, fraudulent charges).

.- Claim B: (…). Facts according to statements of the par-

claimant: A duplicate SIM card has been made without your

consent on 09/03/2020. He declares that he has suffered dis-

positions in your bank account as a result of these events.

guys.

.- Claim C: (...). Facts according to statements of the par-

claimant: A duplicate SIM card has been made without your

consent on 01/22/2021.

During that period of time in which VDF has blocked the card

SIM, various transactions have been made and a credit has been requested.

bank account that you have become aware of through your e-mail.

tronic. In all three cases, the claims have been admissible.

pending processing, however, they have not been subject to accumulation at the

present procedure because the previous investigation actions

that determined the need to initiate this procedure, was oriented

determined, with the greatest possible precision, the facts susceptible to

capable of motivating the initiation of the procedure, the identification of the

person responsible and the relevant circumstances of the procedure

followed to manage SIM change requests, identifying

possible vulnerabilities, without determining the number of re-

registered cries, given the social alarm generated by the realization

tion of these fraudulent practices, since after the entry into force of

Directive (EU) 2015/2366 of the European Parliament and of the Council of

November 25, 2015, on payment services in the market (in vi-

gor from September 14, 2019), the mobile phone happens to have

a very important role in making online payments when necessary

for transaction confirmation, and converts to this device -y

by extension to the SIM card-, in clear objective of the cybercriminals-

you.

Now, the operator argues that these three additional claims are not

should be taken into account as aggravating factors.

Well, as explained in the Motion for a Resolution, those

three claims filed after June 2, 2020,

are not taken into account as aggravating factors, notwithstanding that this government

continuous review of claims filed with the AEPD sample of

undoubtedly an existing problem in the VDF organization

reflected in the Proven Facts.

In short, the application of the aggravating circumstance of article 83.2.a) of the RGPD is

refers to all the previously analyzed aspects, manifest positions,

party in the Proven Facts, to the social alarm generated by the reality

zation of these fraudulent practices and the high probability of

materialization of the risk, without the number of claims being decisive.

presented mations. And this, because what has been analyzed in the

present sanctioning procedure is the data protection policy

implemented by the data controller as a result of various claims

applications filed with the AEPD.

 Number of stakeholders affected:

Nine claims were registered denouncing these facts. VFD

declared XXX cases in 2019.

Fraud cases

dulent

detected

declared

2019

XXX

Total number of te-

mobile telephony (VDF source)

Total number of requests

tutes of change of

SIM card 2019

(VDF source)

% SIM fraud cases

declared dulent

on line number

neas

12,422,064

XXX.XXX

X.XXX%

And although the resulting percentage represents X,XXX %, it is considered

enough for the Agency to ensure the application of the RGPD.

VDF reiterates that the XXX cases cannot be taken into account without

put them in their proper context by alleging a series of circumstances,

in relation to the total of VDF clients, with the total of requests for

duplicate SIM cards and with the number of requests for SIM cards

denied.

In this regard, it should be noted that the AEPD has taken into account the XXX cases

considering them in their proper context taking into account the circumstances

referred to by VDF.

Now then, to greater abundance, what does make clear the reference

of the XXX cases is that VDF is aware that of the total number of requests

Duplication of SIM cards likely to be considered

as fraudulent, which according to VDF's own criteria, would amount to

XXXX in the time period in which the actions of the

present proceeding, XXX, i.e. X,XX % of those requests

of duplication of SIM cards likely to be considered fraud.

slow signals are not detected by VFD, resulting in the presence of a

non-negligible probability of materialization of the risk.

 Level of damages suffered:

Tall. It is true that the verification system of banking entities

responds to the will of these and not of VDF. However, it is also

true, that if VDF ensured the procedure of identification and

ga, the entity verification system could not even be activated.

des banking The scammer after getting the activation of the

new SIM, takes control of the telephone line, thus being able to

nuation, carry out fraudulent banking operations by accessing the

SMS that banks send to their customers as confirmation

tion of the operations they execute. This sequence of events set

evident in the nine claims filed generates a series

serious damages that should have been taken into account in

an impact assessment relating to data protection (considering

do 89, 90, 91 and article 35 of the RGPD). Regarding the return of

refunded amounts, only the return of the amounts is confirmed.

amounts subtracted in the case of claimant four. In defi-

definitive, from the moment a duplicate is delivered to a person

other than the owner of the line or authorized person, the customer loses the

control of the line and the risks, damages, multiply. Ade-

Moreover, the events occur with an overwhelming immediacy.

VDF insists on the degree of responsibility that, in its case,

can be blamed on them, cannot be made to depend on an action of

a third party that escapes their control, that is: the security measures imposed

supplemented by one or another banking entity or even the fact that

the affected party may or may not have electronic banking.

In relation to this allegation, in addition to what has already been indicated above,

the degree of responsibility falls within its scope and not third parties,

noting that the SAN -Administrative Contentious Chamber- of 5

May 2021, establishes that: “On the other hand, regarding the fact that

we are facing the fraud of a third party, as we said in the SAN

of October 3, 2013 (Rec. 54/2012)-: "Precisely for this reason, it is

necessary to ensure that the person who hires is the one who really

claims to be and appropriate preventive measures should be taken to

verify the identity of a person whose personal data is to be

object of treatment".

Regarding VDF's allegation regarding the lack of evidence or assessment

any of the damages actually suffered that have not been compensated

used by the VDF itself or the banking entities, it should be noted

that, only the return of the amounts subtracted is confirmed

in the case of claimant four, there is no evidence of

reimbursement in the other cases of the return of the amounts sub-

brought.

Furthermore, the damages suffered by the claimants

are recorded as Proven Facts in this proceeding

in relation to the claims filed with the AEPD, (withdrawal

of cash from ATMs, carrying out financial operations such as

contracting of loans; making transfers; acquisitions

of various products; contracts for services of the information society

training, etc.); and that, as VDF asserts, there may be a com-

afterthought by the VDF itself or by the banking entities. in

by virtue of a legal obligation, does not imply a reduction in the reproduction

liability of the infringing conduct of VDF, in terms of protection

data regarding the issuance of duplicate SIM cards.

- Article 83.2.b) GDPR:

 Intentionality or negligence in the infringement:

As we already indicated in the Motion for a Resolution, denying the concurrence

evidence of negligent action on the part of VDF would amount to acknowledgment

certify that their conduct -by action or omission- has been diligent. obviously-

te, we do not share this perspective of the facts, since it has to be

given evidence of lack of due diligence. It is very illustrative,

SAN of October 17, 2007 (rec. 63/2006), assuming that it is

of entities whose activity entails the continuous treatment of

customer data, indicates that "…the Supreme Court has understood

that recklessness exists whenever a legal duty of care is disregarded

care, that is, when the offender does not behave with diligence

required. And in assessing the degree of diligence, it must be weighed

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

in the case now examined, when the activity of the appellant is of

constant and copious handling of personal data must in-

insist on rigor and exquisite care to adjust to the precautions

legal obligations in this regard".

Now VDF continues to argue its disagreement regarding the si-

following statement from the Agency: "Similarly, the fact that VDF

has subsequently implemented modifications in the technical measures

existing unique or organizational, corroborates that those others do not pro-

they provided adequate security"; likewise, it indicates that

to make the fact of complying with the RGPD harmful for VDF, and

that if the sanction is imposed for the lack of, in the opinion of the Agency, de-

due diligence, the negligence that constitutes precisely the in-

fractor cannot, in turn, be valued as an aggravating circumstance.

VDF confuses what constitutes the offending type (in this case in relation to

tion with the lack of proactive responsibility) with the pleasant circumstance

vantage of negligence in the infringement. Identifies lack of responsibility

proactive and due diligence implicit in it, with negligence in the

infraction, the latter as an aggravating circumstance of his conduct. Thus, he argues that

lack of due diligence is negligence and assimilates both concepts.

Well, the sanction is imposed for the lack of security guarantees.

treatment of article 5.1.f) of the RGPD and the principle of res-

proactive responsibility of article 5.2 of the RGPD. The offending act

consists in that VDF, as responsible for the processing of the issuance of

duplicate SIM cards has not been able to feasibly demonstrate

that in said treatment has complied with the principles of protection

tion of data collected in article 5 of the RGPD, by not having adopted

the appropriate measures for the protection of the data subject to treatment

Issuance procedure for duplicate SIM cards. especially when such

and as we have indicated in the SAN of October 17, 2007 (rec.

63/2006) mentioned "when the activity of the appellant is of

constant and abundant handling of personal data

has to

insist on rigor and exquisite care to adjust to the

legal provisions in this regard.

Negligence as an aggravating circumstance is then connected, not with the type

fraudster himself (which includes much more than due diligence), but

with events surrounding this, since we find ourselves with a

large company that processes the personal data of its

clients on a large scale, in a systematic and continuous way and that it must ex-

exercise care in fulfilling its obligations in terms of

data protection, as established by case law. maximum

when you have more than enough means of all kinds to

fulfill properly. It is not the same if the offense is committed by

VDF than by a natural person or by a small company. In the first

In the first case, non-compliance is more reprehensible. This is inferred from the

ordinance 148 of the RGPD that imposes being in the concurrent circumstances

to classify an infraction as serious or minor for the purposes of the

GDPR.

In this file, negligence as an aggravating circumstance is perceived, among

others, in the delay in adopting corrective measures once

duced the duplication of the SIM card, since they are

adopted, not after having VDF proof of fraudulent duplicates

of the SIM cards, but after the communication of the AEPD of the

claims filed. Failure to fix vulnerabilities

in time has aggravated the damage to the people affected.

Non-compliance has degrees, resulting in this being more burdensome due to the

circumstances described, fully entering the field of negligence

Inc.

- Article 83.2.d) GDPR:

 Degree of responsibility of the person in charge:

It is considered that the technical and organizational measures implemented

they are insufficient. The personal data that VDF collects both for the

contracting the service as well as during its provision, are your responsibility.

liability and must be treated in a way that allows proper development

the contractual relationship between the parties, guaranteeing at all times

I encourage the application of the principles of article 5 RGPD.

- Article 83.2.e) GDPR:

 Any previous infraction committed by the person in charge:

Procedure No.

Sanction resolution date

Sanction

PS/00139/2020

07/03/2020

PS/00168/2020

07/20/2020

PS/00009/2020

07/28/2020

PS/00186/2020

08/31/2020

PS/00303/2020

10/26/2020

PS/00341/2020

10/28/2020

PS/00348/2020

06/11/2020

PS/00356/2020

11/16/2020

PS/00308/2020

11/16/2020

PS/00415/2020

12/30/2020

9,000.00

45,000.00

48,000.00

60,000.00

36,000.00

30,000.00

42,000.00

42,000.00

36,000.00

54,000.00

PS/00430/2020

02/10/2021

120,000.00

VDF argues that this point was not included by the Agency as a circumstance

aggravating substance in the Start Agreement and shows its disagreement

with this fact, because it was included as an aggravating circumstance when VDF included

in his pleadings brief of March 3, a reference to the fact that he had not

had been sanctioned for violation of articles 5.1 f) and 5.2 of the RGPD

in relation to facts similar to those dealt with in this file.

Also because none of the eleven sanctioning resolutions cited

by the Agency in the Resolution Proposal refer to infractions

tions of articles 5.1 f) and 5.2 of the RGPD in relation to the following facts:

thousands of those treated in this file.

In this regard, it should be noted that the procedure for the Agreement to initiate

sanctioning procedure is carried out in accordance with the evidence

that are available when it is issued and without prejudice to what results from the

procedure instruction; being as a result of what is included in the writing

of allegations of March 3 when as a result of the instruction

tion of the procedure, its inclusion is agreed upon verifying that the

AEPD had issued eleven prior sanctioning resolutions against

VDF.

In relation to the argument that the offenses for which

had been sanctioned VDF did not refer to infractions of the articles

5.1.f) and 5.2 of the RGPD, note that article 83.2.e) establishes that “When

decide the imposition of an administrative fine and its amount in each
individual case, due account shall be taken of: e) any prior infringement
committed by the person in charge or the person in charge of the treatment". The
recital 148 of the RGPD adds that it must refer to "any in-
pertinent previous fraction" or "relevant" of the translation of the original text.
nal in English – "relevant". The procedures listed in the table ex-
put are relevant and are directly related to the current one.
Most of them, also in the one now examined, are produced
starting from an identity fraud not detected by the company, which
entails a treatment without consent of personal data, transferring
personal data to a third party other than its owner and by default
cough in the established data protection model or due to insufficiency
of suitable measures. They show previous breaches in mate-
identity fraud and lack of measures in identity procedures
identity verification.
Regarding the consideration of the provision of article 83.2.e) of the
RGPD as a mitigating factor, as claimed by the defendant, the
SAN, of May 5, 2021, rec. 1437/2020, indicates that: "Considers,
on the other hand, that the non-commission of
a previous offense. Well, article 83.2 of the RGPD establishes
that must be taken into account for the imposition of the administrative fine
goes, among others, the circumstance "e) any previous infraction committed by
the person in charge or the person in charge of the treatment". It is a circumstance
aggravating substance, the fact that the budget for its
application entails that it cannot be taken into consideration, but it does not

does not imply nor does it allow, as the plaintiff claims, its application as a

nuant".

- Article 83.2.g) GDPR:

 Categories of personal data affected:

The personal data affected by the treatment has a specific nature.

sensitive since, as indicated in the Initiation Agreement, "The acces-

Unauthorized use of a duplicate SIM card is considered particular.

serious mind as it enables identity theft. and although not

"special categories of personal data" were affected according to

defines the RGPD in its article 9, this does not mean that the data stolen

two were not of a sensitive nature", since it allows the impersonation

of identity.

The delivery of a duplicate SIM in favor of a third party other than the lender

legitimate owner is considered particularly serious since it makes it impossible to

sending or receiving calls, SMS, or access to data service,

which happens to be in the hands of the supplanting person.

Obtained the duplicate, the path to the applications and ser-

vices that have as a key recovery procedure the en-

sending an SMS with a code to be able to change the passwords. In

In addition, it enables identity theft.

And although they have not been affected "Special categories of data per-

personal” as defined by the RGPD in article 9, this does not mean that the
stolen data were not of a sensitive nature. It's not about the data
personnel required to issue the duplicate card,
if not of the card itself as personal data associated with a line of
telephony owner of a user, which is obtained with the purpose of supplanting
use your identity to obtain access -among others- to the applications
banking or electronic commerce, in order to interact and perform
perform operations on your behalf, authenticating through a user and
password previously taken from that user, as well as with the autho-
double factor authentication when receiving the confirmation SMS in your pro-
own mobile terminal where the duplicate SIM card will be inserted.
- Article 76.2.b) LOPDGDD:
 Linking the activity of the offender with the performance of treatment
personal data:
The development of the business activity carried out by VDF requires
continuous and large-scale processing of the personal data of the
customers. The number of mobile voice telephone lines reported in the
"FOURTEENTH Background" and "SEVENTH Legal Basis-
MO”, positions VDF as one of the telecommunication operators
largest in our country.
Furthermore, when demonstrating the proportionality of the
proposed sanction it should be noted that if the sanctions will be applied
provided for in the previous regulations, taking into account that the infractions
offenses committed by VDF are classified as very serious offenses and the
Article 45.3 of the LOPD of 1999 provided that "Very infractions
serious will be sanctioned with a fine of 300,001 to 600,000 euros pre-

view for very serious infractions” for each of the claims

nes, as there are 9 claims the fine that would have been imposed with

the previous regulation would be between 2,700,000 and

5,400,000 euros, with which the fine currently set would be within

of the range of the sanction provided for in the previous regulations, which is no longer

applicable.

Although it must be made clear, as we have already indicated, that it is not imposed

for those cases in which claims have been filed, but

because these cases highlight the breach of guarantees

in terms of security (article 5.1.f) RGPD) and responsibility

proactive (article 5.2 of the RGPD) that is evident in the definition

science of the security measures adopted by VDF in the treatment

SIM card duplication data storage that allows the issuance

of duplicates fraudulently.

In addition, it must be taken into account that currently the GDPR does not set

a minimum amount and that article 83.5 establishes that “Infringements

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

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

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

as a maximum of the total global annual turnover of the financial year

previous financial statement, opting for the highest amount”.

On the other hand, the following have been taken into consideration, as mitigating factors:

- Article 83.2.c) RGPD:

 Measures taken by the person responsible to mitigate the damages

suffered by the interested parties:

positive. Namely: (...).

- Article 83.2.f) GDPR:

 Degree of cooperation with the supervisory authority:

Tall. The Agency considers that VDF has cooperated favorably

with research, providing a response to all the requirements

cough and takes it into consideration.

- Article 76.2.c) LOPDGDD:

 The benefits obtained as a result of the commission of the investment

fraction.

Obtaining an economic benefit beyond receiving

the price of the cost established for the issuance of duplicates of the cards

SIM card

- Article 76.2.h) LOPDGDD:

 The submission by the person in charge or person in charge, with

voluntary, alternative conflict resolution mechanisms, in

those assumptions in which there are controversies between those and

any interested.

Various telecommunications operators, including

VDF, signed a Protocol with AUTOCONTROL that, without prejudice

of the powers of the AEPD, provides mechanisms for the re-

private settlement of disputes relating to data protection in the

field of contracting and advertising of communications services

electronically, dated September 15, 2017. Protocol whose application

effective cation should be considered as mitigating.

Therefore, in accordance with the applicable legislation and after assessing the graduation criteria

tion of the sanctions whose existence has been accredited, the director of the AEPD,

in accordance with the evidence available in this proceeding

and taking into account the factual background, the proven facts and the grounds

aforementioned legal

RESOLVE

FIRST: IMPOSE VODAFONE ESPAÑA, S.A.U., with CIF A80907397, for a

infringement of article 5.1.f) and 5.2 of the RGPD, typified in article 83.5.a) of the RGPD,

and classified as very serious for prescription purposes in article 72.1.a) of the LO-

PDGDD, a fine of 3,940,000.00 euros (three million nine hundred and forty thousand euros).

ros).

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

THIRD: Warn the sanctioned party that he must make the imposed sanction effective once

Once this resolution is enforceable, in accordance with the provisions of art.

Article 98.1.b) of the LPACAP, within the voluntary payment term established in Article

68 of the General Collection Regulations, approved by Royal Decree 939/2005, of

July 29, in relation to article 62 of Law 58/2003, of December 17, me-

upon admission, indicating the NIF of the sanctioned person and the number of the procedure that

appears at the top of this document, in the restricted account number ES00

0000 0000 0000 0000 0000, opened in the name of the AEPD in the banking entity CAI-

XABANK, S.A.. Otherwise, it will be collected in the execution period.

vo.

Received the notification and once executed, if the date of execution is

between the 1st and 15th of each month, both inclusive, the term to make the payment

will be until the 20th day of the following month or immediately after, and if

is between the 16th and last day of each month, both inclusive, the term of the payment

It will be valid until the 5th of the second following month or immediately after.

In accordance with the provisions of article 50 of the LOPDGDD, this

Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with article 48.6

of the LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the

Interested parties may optionally file an appeal for reconsideration before the

Director of the AEPD within a month from the day following the notification

cation of this resolution or directly contentious-administrative appeal before the

Contentious-administrative Chamber of the National High Court, in accordance with the provisions

placed in article 25 and in section 5 of the fourth additional provision of the Law

29/1998, of July 13, regulating the Contentious-administrative Jurisdiction, in the

period of two months from the day following the notification of this act,

in accordance with the provisions of article 46.1 of the aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of article 90.3 a) of the LPACAP,

the firm resolution may be suspended in administrative proceedings if the interest

sado expresses its intention to file a contentious-administrative appeal. Of being

In this case, the interested party must formally communicate this fact in writing

addressed to the AEPD, presenting it through the Electronic Registry of the Agency

[https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other

records provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. Also

must transfer to the Agency the documentation that proves the effective filing

of the contentious-administrative appeal. If the Agency were not aware of the information

filing of the contentious-administrative appeal within two months from the

day following the notification of this resolution, the suspension would end.

precautionary statement.

Sea Spain Marti

Director of the AEPD

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es