 Procedure No.: PS/00021/2021

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: On November 27, 2019, the director of the AEPD, before the news appeared in the media regarding the use of fraudulent practices dulent based on the generation of duplicate SIM cards without the consent of their legitimate owners in order to access confidential information for purposes (known as “SIM Swapping”), urges the General Subdirectorate of Ins-Data Collection (hereinafter, SGID) to initiate ex officio the Prior Actions of Research aimed at analyzing these practices and existing security measures. you for its prevention.

Namely:

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

SECOND: A.A.A. (hereinafter, the claimant party one), on December 12 of 2019, files a claim with the General Registry of the Regional Council of ***LOCATION.1, which is registered with the AEPD on December 13, 2019, directed against TELEFÓNICA MÓVILES ESPAÑA, S.A.U., with CIF A78923125 (in hereinafter, TME), for the following reasons:

“On 03/06/2019 a duplicate of the ***TELÉFONO.1 SIM card was made in the state-

establishment of THADER TELECOMMUNICATIONS of ***LOCALIDAD.2, without my consent.

feeling, at 18:45:41. Through this duplicate they have been able to access my

bank account, hurting me financially. I request that you sanction this use

lization of data without consent.

Together with the claim, it provides the complaint filed for these facts, on the 8th of

March 2019, with procedure number ***DILIGENCIA.1 extensions of the diligence

***DILIGENCIA.2 -related to another complaint previously filed by some

similar events-, before the Mossos d'Esquadra USC of ***LOCATION.3 (Barcelona)

in which he denounces that: "(...) they have duplicated the SIM card of his mobile ***TE-

LÉFONO.1 and this time, they have accessed their BBVA online banking and have made two

transfers for a total value of 28,000 euros. (...) That the final current account that

receives the transfers is the ES00 0000 0000 0000 0000 0000 of BBVA in the name

of B.B.B.. (…) That precisely, since the afternoon of March 6, 2019, the de-

complainant was left with the mobile inoperative. (…) That it will present a claim to

Movistar for this reason also since it is the second time that they perform a duplicate-

do of your SIM card without your authorization or physical ID.”

Also, provide a copy of the email sent from the email address ***EMAIL.1 to

TE_COMMERCIAL SUPPORT, with the following tenor:

"Good,

This client comes for the first time on 02/07, they had called him from ***PRO-

VINCIA.2, that a man went around the shops wanting to make a duplicate of his li-

na. And that he thought he no longer had a line on ***PHONE.2, evidently, in-

sections in CTC and they had done it from MOVISTAR CARREFOUR ***PROVIN-

CIA.1 A DUPLICATE ON 02/5/2019.

He lives in ***LOCATION.4, a town near ***LOCATION.3, in the province

from Barcelona.

WE MADE a duplicate of ***PHONE.2 again and apart from that we made a new number.

vo, which is ***TELEPHONE.1, the client went to the bank and in exchange (sic) the number of

contact for the new on all sites, just in case. But the surprise was that

yesterday at 18:45 they did the same thing again, a DUPLICATE (sic) but of the number

new, the ***PHONE.1 and this time they have used it to empty 28,000 euros of

your bank account.

Demand that you always be asked for your ORIGINAL DNI AND A PASSWORD TO DO

ANY PROCESS, BY PHONE OR IN STORE. put a note

IN CTC REPORTING IT. and above all he wants to be calm that if it is not the na-

die can do anything in your name

And he demands that the two duplicates be returned to him on the invoice, since it is a matter of a

movistar worker who is making duplicates without asking for original identity.

The client wants to know this time if it has also been in the Carrefour of ***PROVIN-

CIA.1, but since they did not enter CTC, YESTERDAY'S HISTORY does not appear and I

It won't let me see who made the duplicate.

I ATTACH THE FIRST COMPLAINT, THE FIRST DUPLICATE AND THE REGISTRATION OF THE

NEW NUMBER THAT WE DID ON 7/02.

THE DUPLICATE INVOICES OF DAY 7/02 AND DAY 7/03 FOR YOUR DE-

RETURN AND PROOF OF THE BANK WHERE THE NAME APPEARS

BRE OF THE PERSON WHO HAS MADE THE IDENTITY THERAPY.

AND THE AMOUNTS THAT HAVE BEEN TAKEN AWAY.

ID I SIGNED CONTRACTS."

It also provides a screen print of the duplicate SIM card issued

on March 6, 2019, regarding the subscriber number ***PHONE.1.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/106

On December 16, 2019, claimant one, filed a new brief

before the General Registry of the Regional Council of ***LOCALITY.1, which is registered

in the AEPD on December 17, 2019, through which he submits a complaint

presented on February 7, with procedure number ***DILIGENCIA.2 before the

Mossos d'Esquadra USC of ***LOCATION.3 (Barcelona) in relation, on the one hand,

to an identity theft attempt in 5 Movistar stores in

*** PROVINCE.2 to obtain a duplicate of your SIM card regarding the number of

subscriber ***TELÉFONO.2 and on the other hand, in relation to the issuance of a duplicate

of your SIM card on February 6, 2019, at a Carrefour in ***PROVINCIA.1.

Regarding this last issue, it provides the distributor code ***CODE.1 and the

number of the agent responsible for said expedition: ***AGENTE.1.

It also provides a screen print of the duplicate SIM card issued

on February 5, 2019, regarding the subscriber number ***PHONE.2.

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 January 22, 2020, the claim was transferred to TME and to

THADER TELECOMMUNICATIONS, S.L. (hereinafter referred to as THADER), so that

give their analysis and respond within a month.

In response to said requirements, THADER stated -among other arguments-

the next:

"(…) 3 — Report on the causes that have motivated the incident that has originated

do the claim:

On 03/06/2019 a customer visited our Movistar store located in

ADDRESS.1 of ***TOWN.2 (PROVINCE.2), requesting a change

SIM card of the number ***PHONE.1 providing this documentation:

~

~

Photocopy of the DNI of the holder of the line.

Photocopy of the complaint for theft of the DNI holder of the line and mobile with the number

mere ***PHONE.1.

~

Authorization signed for its management.

~

Photocopy of the passport of the authorized person.

Validating the documentation provided, the SIM card is changed

according to Movistar's operations in the Authorized to traditional section".

According to Art. 6 of RGPD Lawfulness of Treatment

I.A The interested party gave his consent for the processing of his personal data-

them for one or more specific purposes.

I.B The treatment is necessary for the execution of a contract in which the inter-

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

them.

4 — Report on the measures adopted to prevent incidents from occurring.

similar ties, dates of implantation and controls carried out to verify their

effectiveness

In view of the way of acting to produce this type of fraud or opt-in swapping

We agree to accept the identification of the holder on the SVIC option (scanner),

only the original and valid DNI being valid and in the presence of the holder, leaving the

other validation options not suitable.

We implemented these measures on 01/24/2020, by our own decision, by

our DPD and on the recommendation of our headquarters about similar frauds de-

tected at the national level "Annex 2".

We proceed to the daily control of SIM card changes with strict documentation.

channeled in SVIC.

5 — Any other that you consider relevant

The company in its procedures implements training for its dependency on

LOPD and RGPD to staff via training.

Request to the head office to inform us of similar causes of fraud at a national level.

nal.

We put at your disposal our record of activities, security document,

ity 2016 with respect to LOPD 15/1999, files registered prior to coming into force

GDPR compliance and permanently updated activity log to de-

show collaboration and proactive responsibility from the beginning

tes and after the entry into force of the EU regulation 2016/679 by this

address.

ATTACHED DOCUMENTATION

Annex 1 Extract SIM duplicate identification bulletins

Annex 2 Mail Responsible for Movistar on fraud

FICHE DEFI THADER TELECOMMUNICATIONS S.L

THADER TELECOMMUNICATIONS SECURITY DOCUMENT

INTERNAL AUDIT THADER TELECOMMUNICACIONES, S.L

RGPD MANUAL THADER TELECOMUNICACIONES, S.L"

For its part, TME did not respond to this request, notified on the 27th of

January 2020, through the Electronic Notifications and Electronic Address Service.

nica Enabled, according to the certificate that appears in the file.

On said claim fell resolution of ADMISSION TO PROCESS dated 30 of

March 2020, in the file with no. of reference E/00560/2020.

THIRD: C.C.C. (hereinafter, the claimant party two), on March 6,

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

reasons:

“On February 13, 2020, I was the victim of fraudulent SIM card duplication in

the CATHOME store in ***LOCALIDAD.4 (Barcelona) which is a distributor of Tele-

Movistar phone.

This information (SIM duplication and location) is provided by Telefónica

when I called to ask what was happening with the service when I realized that I did not have-

I didn't have access to the network.

Consequence of fraudulent duplication, carried out by means of impersonation

of identity, was the theft of 18,000 euros in my bank accounts at Banco San-

tander.

I called CATHOME and Movistar Customer Service several times

to gather more information on the details of how the event happened, but everything

they were evasive. At CATHOME they told me to wait and see what they could tell me.

About 5 hours later they send me an SMS (I had already recovered my number

telephone) from which it follows that they recognize that the fact of the

duplication but wait longer, to date, they have not been put back

in contact with me. How was the process of identifying the thief carried out? (me

I never lost my ID or my credit cards)

Is there a mandatory protocol to carry out a duplication of tar-

SIM card? Did the store follow protocol? Is this protocol adequate in relation to

to the risk that is run?

In my opinion, a little research can be done to make sure that the person

who asks for the duplicate is who he says he is and many of the crimes that can be

commit with this class of methods would be nullified, so I think there is

a clear SECURITY GAP and this is one of the reasons why I pre-

I feel this claim.

It is important to keep in mind that it is not just people's money that is at risk.

While the fraudulent mirroring is active all calls, messages etc. You

they reach the criminal putting the security of the victim's contacts at risk.

In my case, the thief took the calls made to my phone number.

I myself, got to talk to him. If he just wanted to steal money, why did he take the

calls?

I also put this claim so that, if it were the case, they sanction the store

CATHOME and/or Telefónica Movistar. (...).”

Along with the claim, he provided two complaints filed with Post P. de las Ro-

of the Madrid Civil Guard Command, on February 13, 2020,

with certificate number ***ATESTADO.1 and dated February 18, 2020, with number

number of attestation ***ATESTADO.2.

In the first of them, he denounces that:

”(…) a duplicate of the SIM card of the telephone ***TELÉFONO.3 no

authorized by the complainant, that the complainant about 1:00 p.m. when making a

call from your phone this does not allow you to make it.

That he begins to take steps, he gets in touch with TELEFONICA MOVIS-

TAR which inform you that you have made a duplicate card IN A STORE-

DA DE MOVISTAR located at ***ADDRESS.2 of the town of ***LOCATION.5.

That the complainant informs him that he is in Madrid and it is impossible for him to

have authorized any duplicates.

That having well-founded suspicions that this was not normal, he performs checks

deposits in your bank account of BANCO SANTANDER which is at your

name, observing several unauthorized charges in it, these being the following:

following:

They have made a purchase in the REVOLUT company worth 2,500 euros

They have made a purchase from the REVOLUT company worth 3,500 euros.

(...) that he received a message on Monday, February 3 from his bank from (...) his account manager

Santander bank asking him to contact the telephone number ***TELÉ-

FONO.4 and that on the 10th he received a call from the Bank's anti-fraud department

Santander informing him that there was an attempt to manipulate accounts from

***COUNTRY.1, who went to the bank and changed the passwords."

In the second of them, he denounces that:

"(...) you want to expand the data of the charges suffered on your card since they have made you

filed more charges of which he was not informed the day he made the complaint.

That on February 13, 2020, when he was reviewing his accounts, he observed that they had

made some charges which you have not made or authorized in your bank account

***ACCOUNT.1 and associated card number ***ACCOUNT.2, for a value of:

REVOLUT company, 02-13-2020, worth 2,500 euros

REVOLUT Company, 02-13-2020, for a value of 5,500 euros

That same day they have carried out the same procedure in another account that has

connects with the bank ***ENTIDAD.1 associated card number ***TARJE-

TA.1, for a value of:

REVOLUT Company, 02-13-2020, for a value of 2,450 euros

REVOLUT Company, 02-13-2020, for a value of 3,500 euros"

On June 8, 2020, the claim was transferred to TME, so that it could process

give its analysis and give an answer within a month.

In response to said request, TME stated -among other arguments- the following:

following:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

7/106

“(…) 3. Report on the causes that have motivated the incidence that has originated

the

claim.

In relation to the claimed facts, TME informs that there is a request for

change of ICC of the Claimant's SIM card on February 13, 2020 at

11:48 a.m. to 2 through one of our (...), and specifically, from the (...) ***LOCA-

LIDAD.4”.

Reviewed the case and despite the fact that TME has an adequate and well-known operation

by all our agents on how to act in the event of a request to change the tar-

SIM card and that will be detailed later, in this particular case it has been possible to

determine that (...).

That same day at 5:12 p.m., as the Complainant explains in his brief of

claim, another ICC change is requested to get your line back. This application

is done in the (...), which is attached as Annex 2. As it was transferred in the

framework of the information requirement with ref. ***REFERENCE.2 of the AEPD,

TME has an adequate procedure for changing SIM cards. (…)

Therefore and in conclusion, in this specific case in which it has been affected

only one person has been able to determine that (...).

4. Report on the measures adopted. Indicate that all brand personnel

Movistar is required to access and comply with all procedures established

two to make and deliver SIM duplicates through our (...). Therefore, it

they have made reinforcements and reminders of the operation of changes of duplicates

of SIM, as well as the publication of a communication of awareness and sensitization

information about SIM card changes. (…)"

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

September 2020, in the file with no. of reference E/03543/2020.

FOURTH: In view of the facts denounced by claimants one and two,

of the documents provided and the Internal Note agreed by the director of the

Agency, the SGID proceeded to carry out preliminary investigation actions

for the clarification of the facts in question, by virtue of the investigative powers

authorization granted to the control authorities in article 57.1 of the Regulation (EU)

2016/679 of the European Parliament and of the Council, of April 27, 2016, regarding the

protection of natural persons with regard to the processing of personal data

them and the free circulation of these data and by which Directive 95/46/EC is repealed

(General Data Protection Regulation, hereinafter RGPD), and in accordance

with the provisions of Title VII, Chapter I, Second Section, of the LOPDGDD.

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

information services addressed to TME, on different dates:

Secure Verification Code Requirement

C/ Jorge Juan, 6

28001 – Madrid

Required date

I lie

Notification date-

tion required

I lie

www.aepd.es

sedeagpd.gob.es

8/106

01/13/2020

03/06/2020

06/29/2020

09/17/2020

01/15/2020

03/09/2020

07/06/2020

09/21/2020

First

Second

Third

Fourth

CSV.1

CSV.2

CSV.3

CSV.4

In the first of the requirements, dated January 13, 2020, the following was requested:

following 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 March 6, 2020, the same information cited in the previous request, dated January 13, 2020.

In the third request, dated June 29, 2020, the following information was requested:

training:

POINT 1

Clarification is requested on the following aspects in relation to the answer-

tion of our request dated March 6, 2020, within the framework of this

same file:

A). In the case of the MOVISTAR brand, it is indicated that it is only possible to request

face-to-face in store. Information is requested on whether in any exceptional case

Transact by phone or online, always talking about private clients

(residential)

In the affirmative case, a copy of the written procedure is requested where the

all cases that are processed remotely, including all sub-

positions or circumstances.

If so, a copy of the specific instructions given to the

operators with detailed information on how the operator values all the sub-

positions, including how you must assess the client's circumstances to access

der to telephone processing.

B). In the case of authorizations or representations for preliminary procedures

essential in store, information is requested on the controls that are carried out on

the copy of the identity document (of the client who authorizes or represented).

Information on whether the image of the identity document is stored

of the applicant, the authorization or accreditation of representation, and the copy of the document

customer document.

C) In home deliveries, information is requested on the express possibility

of the change of the delivery address of the SIM, both during the request for

change of SIM, as prior to the change of SIM in independent management

te, and on the controls established to make the change of this data.

D). In O2 and TUENTI Information on the controls established to process

changing a user's email address.

Implications that a change of email address can have in

the

Fraudulent request or activation of a new duplicate SIM. Information on-

See if the email address matches the user code

for apps/webapps, or if it is used during the SIM change process.

AND). For the cases of delivery of the SIM by (...), or courier companies:

The verifications that are carried out in the home delivery of the card are requested.

ta SIM for recipient identification. Copy of contracted documentation

with the courier companies that carry out the distribution, where the

identity checks or instructions in this regard to be carried out by the

splitter.

POINT 2

List of 20 cases of SIM duplicates claimed as impersonation of

identity or fraudulent by customers, of the MOVISTAR brand. The list in-

will include SIM duplicates requested from January 1, 2020, that is,

all those claimed that happened from January 1, from the first,

consecutively up to 20.

It is requested to indicate in the list only:

- the date of the SIM change,

- the line number,

- request channel,

- delivery channel.

POINT 3

On cases presented before this Agency that are summarized in the table (which is

fully reproduced in this act of procedure):

It is requested:

A) Reason why the duplication of SIM was possible for each case. accredits-

tion of the controls that were passed, for each case, on the identity of the

citation in the face-to-face application in the store. Copy of identity document

submitted and controls that were passed, or result of validation with codes

go QR .

B) Reason why two consecutive SIM duplicates were possible for

This Customer. Information about the type of customer contract.

C) Actions undertaken by the entity in each case, including accreditation

documentation of the following aspects:

~

If the client has been marked as a victim of fraud to avoid possible in-

future phishing attempts.

~

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

the point of sale.

~

If changes have been made in the procedure to avoid future cases if

thousands.

~

If any action has been taken with the distributor or store.

~

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

solution of your case.

In the fourth and last of the requirements, dated September 17, 2020, it was

requested the following information:

1

POINT

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

11/106

On the list of 20 cases of SIM duplicates denounced/claimed (which

is fully reproduced in this act of procedure):

A. In the cases of application and face-to-face delivery, a copy of the DNIs or documents is requested.

identification elements provided by the SIM change applicants.

B. For cases of telephone request:

~

Copy of the recording of the conversation where the applicant exceeds the policy

of security.

~

Detail of the circumstances that concurred to access the procedure-

tion of the telephone request.

C. General information on the casuistry of “misappropriation of the SIM”:

~

Specific information on whether the SIMs were stolen from a point of sale or

How did this misappropriation occur?

~

Information on whether it is possible to acquire SIMs without associating them to any line or

client. Causes for which a customer is allowed to take a product from a store

SIM not activated and not associated with a specific line, and is allowed later.

mind activate said SIM by telephone and associate it with a line.

Information if this possibility exists, without SIM swapping fraud, consistent

in the activation of a SIM that is in the possession of a client, without having been

previously associated in the entity's systems to a line owned by it.

dad.

~

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

Any SIM for a given line. (Case of possible stolen SIMs

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

~

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

it is not associated with a line or client during its collection.

FIFTH: On March 10, 2020, TME requests an extension of the term before

the impossibility of gathering and structuring the required information within the established period

do.

On March 12, 2020, the Deputy Director General for Data Inspection

agrees to extend the term to respond for a period of five days, from

the day following the day on which the first term granted expires.

SIXTH: In response to the four requests formulated, TME provides the following

information, which was analyzed by this Agency:

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

of SIM card:

Movistar brand customers

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

12/106

(...).

2.- Detailed information on the procedure:

(...):

MOVISTAR Brand:

(...).

O2 BRAND

(...).

TUENTI BRAND

(...).

3.- Instructions given in this regard to the personnel who attend to the requests:

(...).

4.- Information on whether the performance of the controls is reflected:

Movistar brand.

(...).

O2 brand.

(...).

Tuenti brand.

(...).

5.- Reasons why identity theft has been possible in some cases.

number of clients:

(...).

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

The representatives of the entity have stated that they will develop the following actions:

nes about it:

(...).

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

throughout the year 2019.

(...).

The total number of clients of the Movistar, Tuenti and O2 brands at the end of January

2020 was 8,142,352 customers.

Regarding the information requested regarding the additional cases not presented

before this Agency, states the following:

(...).

for the SIMs requested as collected in person at the store, the representatives

Many of MSDs manifest:

(...).

Recording of the conversation is required for telephone cases, in which the

applicant exceeds the security policy, they do not provide them, stating the representatives

representatives of the entity the following:

(...).

TME has been asked for details of the circumstances that concurred to access

right to the processing of the telephone request, not responding the representatives

of the entity why it was processed by telephone, indicating that in 5 of the cases:

(...).

TME has been asked for information on whether it is possible to acquire SIM cards without

associate them to any line or client as well as the reasons why they are allowed

that a customer takes from a store a SIM without activating and not associated with a line

determined, and it is later allowed to activate said SIM by telephone and associ-

tie to a line The representatives of the entity have replied by providing the following

following information:

(...).

Regarding the information requested regarding the cases presented before this Agency,

company, stated the following:

 File E/00560/2020:

The first duplicate, of the line ***TELÉFONO.2, was never carried out when

complete, since the distributor did not deliver the SIM card to the supplant-

pain The commercial agent who attended the request detected that the documentation

provided by the impersonator did not pass the (...) and the SIM card that was used

to make the continuous duplicate in the dealer's shop. They provide photography

of the SIM card, indicating that its ICC number (XXXXXXXXXXXXXXX)

matches the one assigned to the line. They provide screen printing with the ICC

assigned.

According to statements made by TME representatives in the second case (during

line ***TELEPHONE.1), the duplication was possible due to the concurrence

ence of the following circumstances:

(...).

About the reason why two consecutive SIM duplicates were possible

for this client. Information on the type of contract of the client, the represen-

many of the entity have stated that

(...).

Subsequently, the case is referred to (...), who investigates the assumption to clarify

rar what happened and transfer the conclusions of his study to (...).

In this case, these measures were not implemented because (...).

TME representatives indicate that in case (...). Research studies

The Fraud Prevention program helps us to define new models or scenarios.

fraud, in order to strengthen our operations and better in a cons-

both the security measures implemented and the identification processes of

customers.

(...).

They indicate regarding the internal investigations to clarify the facts that

when there has been evidence of the case, it has been consulted internally in all

two TME systems the different actions on customer lines

to clarify what happened.

Likewise, the usual territorial interlocutors have been contacted to

put them on notice, gather more information and reinforce operations with the

stores involved.

As for carrying out any action with the distributor or store, ma-

They state in general that with the entire network of stores they have carried out

various reinforcements on (...), as well as of (...). When they are aware of

some case of SIM SWAPING (...).

In relation to the changes made in the procedure to avoid cases

future, indicate that (...).

Finally, answering the question of whether they have contacted the client, they indicate

what, (...).

 File E/03543/2020:

They do not provide ID or SIM change request document. They represent-

TME officials have stated that, after reviewing the case and despite the fact that TME has

with an adequate operation and known by all the agents on how to act

act before a request to change the SIM card, in this particular case it is

has been able to determine that (...).

On the same day, the claimant requests another change of ICC to recover their limit.

na.

This request is made in (...), and in this case the TME operation was followed

(...), which are attached.

They indicate that all the staff of the Movistar brand (...).

SEVENTH: D.D.D. (hereinafter, the three complaining party), on October 23,

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

reasons:

“On 09/25/2020 at 2:40 p.m. I receive an email from Movistar telling me

that my Movistar Cloud service had been terminated, so I responded to the

14:53 saying that I had not canceled anything and that it was a mistake or an unauthorized use-

twisted (…)

On 09/25/2020 at 2:58 p.m. I call Movistar 1004 to try to clarify the cancellation,

but as usual I can not contact anyone and the call is cut. Gave-

This call lasted 4 minutes 17 seconds and all this data was recorded on my mobile.

That same day and in the afternoon I noticed strange things on my mobile, I had a message

that "the mobile was lost" and after 8:00 p.m. it no longer had a signal and could not

make or receive calls. I literally panicked as I strongly suspected

I state that my mobile had been hijacked (hacked) or similar. helped by me

wife with her cell phone (which is not from Movistar) and the landline we started a series of calls

distressing calls to my banking entities to block everything. in parallel and

from the landline I called XXXX and although it took me several minutes I managed to explain what

It was happening and I desperately requested that they cancel my mobile number before the confirmation

Banco Santander that my account had already been robbed and they had charged me

fraudulent credit card transactions. My surprise and outrage was indescribable.

ble when they told me that they couldn't do anything since that number, mine ***TE-

LEPHONE.5 (and all the rest of the contract) were in someone else's name.

When I managed to block all the bank accounts, I called Movistar again and

They also told me that they couldn't do anything and that in order to clarify what had happened and

to get my signal back (deactivate the impostor's SIM and activate mine) I would have to go to

a Movistar store. (…)

At 10:00 a.m. on 09/26/2020 I went to the Movistar de las Rozas store near

cana to my home and although they knew me perfectly as a regular customer

They said they couldn't do anything since my mobile (and other services) were

someone else's name and they provided me with a document as proof.

They sent me to the Telefónica central in Gran Vía to unblock the situation

(…)

I was in the Gran Vía premises from 11:00 a.m. to 1:00 p.m. approximately.

and I provided the aforementioned fraudulent document, my monthly receipts

of Telefónica Movistar in pdf on a USB key from 1998, as well as a copy on paper

pel of the last receipt from Movistar. Given the evidence of tests, Movistar decided

cancel the fraudulent SIM and activated mine.

The conclusion of Movistar itself was very clear: the impostor fraudulently changed

mind the contract in your name (possibly by telephone according to Movistar although

unconfirmed) and then went to a Movistar store where he asked for a duplicate of the

SIM. He did not find problems since in the store's computer it was in his name.

opened and later canceled the other one, mine, and it already entered my bank accounts. The

The procedure was relatively simple: he entered my account with my ID (possibly

mind got it from my contract) pressed "lost or forgotten password" and in those

cases the bank sends SMS with security codes that once entered with

They correctly give access to passwords, etc. (…)

Conclusion: Movistar changed my Movistar Fusión contract (fixed, mobile and television)

in the name of another person (...) without protecting my data, which also gave rise to

a scam of XXXXX euros."

Along with the claim, provide the email received on September 25

of 2020 and the response; copy of the repair order dated 09/26/2020; and two

complaints filed before the P. de las Rozas Post of the Guard Command.

Civil Day of Madrid, on September 28, 2020, with certificate number XXX-

XXXXXXXX and on October 2, 2020, with certificate number XXXXXXXXX-

XXX.

In the first of them, he denounces that:

"A total of three charges have been made on the due card, subtracting

a total of XXXX euros.

A total of six charges have been made to the debit card, subtracting a total

of XXXX euros.

They have also made a transfer to him through BIZUM of 500 euros, destined for

swam to a certain E.E.E. with telephone number ***TELÉFONO.6 and a bank recharge-

ria of XXXX euros.

All this makes a total of XXXX euros.

The complainant states the possible modus operandi of the author: That through a

of a change of name of the holder in his contract, for the line belonging to the number

number ***TELEPHONE.5, with MOVISTAR by telephone, without your consent, the

The possible author made the change, requesting a SIM card from said company. nullifying

the complainant's SIM card.

That after obtaining said SIM card, the author made the bank transactions through

through a mobile phone, because after carrying out any operation with the entity

banking entity, you need the approval via SMS of the telephone number that makes the

operation.

After this, the possible author got into the application of the Santan-

der and through I HAVE FORGOTTEN MY PASSWORD, said bank sends SMS to

phone number associated with the bank account.

That the change of holder of the MOVISTAR account, the complainant provides data

of the possible author: F.F.F. ***NIE.1.

It also provides a bank transfer of XXXX euros that was cancelled, which was

addressed to a certain G.G.G.(…).

That the complainant provides the fraudulent MOVISTAR contract with the name and

surnames of the alleged perpetrator, copy of the last invoice of the legal contract of the denouncer,

customer, details of the aborted transfer and the charges made."

In the second of them, he denounces that:

"(…) That on Thursday 10-01-2020 the complainant appeared at his office in the

Banco Sabadell located in (...) to recover the passwords previously blocked for

be able to operate.

That Banco Sabadell reported that unfortunately a transfer had been issued

fraudulent payment amounting to 7,003.00 euros in the name of H.H.H. to the account

ES00 0000 0000 0000 0000 0000 of the banking entity ING reason for which

is forced to report the facts in order to recover the amount defrauded.

The complainant expresses the possible modus operandi of the author", where he reproduces the

same manifestations reported in the previous complaint.

On November 25, 2020, the claim was transferred to TME, so that

proceed to its analysis and respond within a month.

In response to said request, TME stated -among other arguments- the following:

following:

"(…) 3. Report on the causes that have motivated the incidence that has originated

the claim.

Mr. D.D.D. In the document filed with this Agency, he indicates that he is a client of the

Movistar commercial brand with which it has contracted three lines, one fixed and

two mobile lines that are ***PHONE.6, ***PHONE.5, ***PHONE.7.

Likewise, he indicates that on September 25, 2020, he noticed that his line

***PHONE.5 was without service, after this, he contacted our service

customer service at number 1004, where they told him that all his lines

They were in someone else's name.

Subsequently, on September 26, 2020, the client appeared at a

of our physical stores, where they explained that it was possible that a third party

person would have changed the ownership of their lines requesting in turn a duplicate

cation of your SIM card for mobile lines.

In this sense, we have to say that, in this specific case, on September 25,

In 2020 there was a change of ownership in the three lines mentioned above.

subsequently through (...); that same day, the impersonator requests a duplicate tar-

SIM card for mobile lines, but it only makes the change in the line effective

***PHONE.5.

Regarding the cause that has produced the claim, we must indicate that

(...).

In this regard, we inform you that Telefónica has a conventional procedure

solid and adequate verification of the identity of our clients that covers

of sufficient guarantees to identify the applicant for the change of ownership before

to proceed with its processing. In this verification procedure

identity are requested, in addition to (...).

Notwithstanding the foregoing, Telefónica works continuously to improve the measures

available in order to avoid identity theft in the

different contracting processes and subsequent procedures requested by the holders

of the services through the different channels available to it. Thus,

the different processes have been reinforced, which we will detail in the following point.

In relation to the events described, this company reports that the events de-

announced have already been treated and resolved prior to the entry of the

complaint to the Data Protection Agency.

Regarding the actions carried out by Telefónica in the resolution of the

claim raised, we confirm that:

 As of the date of this writing, the lines are regularized in the name of the

original owner, today claimant, Mr. D.D.D.

 The affected line ***TELÉFONO.5, has a new SIM card associated with

correctly assigned to the owner of the line.

 Our Fraud prevention team has contacted the owner to

inform you about the change of SIM card of the line ***PHONE.7 that re-

It is necessary to carry out to regularize it as well.

4. Report on the measures adopted to prevent incidents from occurring

Similar.

During 2020, the following specific measures have been implemented that

affect channel operations:

(...).

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

January 2021, in the file with no. of reference E/09638/2020.

EIGHTH: On August 27, 2020, information was obtained from the Commission

National Markets and Competition on mobile voice lines

by type of contract and by segment, the results being:

OPERATOR

PREPAID

Movistar

Residential

1,215,667

Business

0

POSTPAID

Residential

10,048,727

Business

5,102,197

NINTH: On January 27, 2021, commercial information is obtained on the

sales volume of TME during the year 2019 being the results of

4,340,283,000.00 euros. The share capital amounts to 209,404,687.00 euros.

TENTH: On February 11, 2021, the director of the AEPD agrees to initiate a

sanctioning procedure against TME, in accordance with the provisions of articles 63 and

64 of Law 39/2015, of October 1, of the Common Administrative Procedure of the

Public Administrations (hereinafter, LPACAP), for alleged infringement of article

5.1.f) and 5.2 of the RGPD, typified in article 83.5 of the RGPD and in article 72.1.a) of

the LOPDGDD as very serious, and may be sanctioned with an administrative fine

of 2,000,000.00 euros (two million euros), without prejudice to what may result from

The instruction.

On February 15, 2021, through the Electronic Notification Service and

Electronic Address Enabled, the Initiation Agreement is notified.

ELEVEN: On February 17, 2021, TME requests the extension of the term

to adduce allegations and provide documents or other evidence, and the referral

sion of file PS/00021/2021 and the rest of the referenced files.

TWELFTH: On February 17, 2021, the instructor of the procedure

agrees to the requested extension of the term up to a maximum of five days and dated 23

February 2021, the referral of the copy of the file, in accordance with the provisions

to in articles 32.1 and 53.1 a) of the LPACAP.

THIRD

TENTH

: On February 22, 2021, TME communicates the modification

of the postal address for the referral of sanctioning file PS/00021/2021 and

of the rest of the referenced files.

FOURTH

TENTH

: On February 22, 2021, TME is notified of the Agreement of

extension of the term and dated February 25, 2021, the remission of the copy of the ex-

pending.

FIFTH

TENTH

: Dated March 8, 2021, it is received in this Agency, in

time and form, written by the representative of TME, by which it is proceeded to formulate

allegations and in which, after expressing what is appropriate to his right, he requests:

"Yo. The present procedure is suspended and the claimants are required to

that they provide the status of the complaints filed, as well as the con-

had of the criminal procedures that in his case are under way,

in order to determine if there is criminal prejudiciality.

ii. Subsidiarily and in the event that the request for suspension is not accepted

sion, declare the non-existence of responsibility on the part of TME for the pressures

alleged infractions imputed to him in this procedure, ordering the ar-

subject of this sanctioning file.

iii. Lastly, in the event that none of the previous claims are upheld,

subsequent, that the sanction initially proposed by virtue of art. 83 of the

GDPR."

In summary, in the pleadings he stated that:

PREVIOUS: ON THE INITIATION OF THE PUNISHING PROCEEDINGS.

Considers that the sanction is disproportionate in relation to the facts

affected, which violates the principle of good faith and legitimate expectations that

must govern the activity and the exercise of the functions of any public entity.

ca, as stipulated in article 3.1.e) of Law 40/2015.

On January 20, 2020, the AEPD convened a working group (GT) with different

operators, as well as with other representatives, with the aim of "analyzing

the problems of the duplication of SIM cards and study ways and procedures

measures to prevent their occurrence", convening the first meeting on 4

December 2020.

However, the AEPD decides to initiate a disciplinary proceeding with a pro-

unprecedented sanction.

In addition, the type of offender that had been habitually charging in the cases changes.

those in which, breaking the technical and organizational measures established

given by TME, the fraudsters managed to supplant the identity of the

clients with different purposes (art. 6.1, lack of legitimacy in the treatment

of the data of the interested parties), and that it was the reproach that in any case had

revealed so far in relation to SIM Swapping, but

that, in addition, imputes to TME the responsibility of the result of the fraud carried out

zed by a third party, that is, the result of the theft of money from the accounts

bank accounts of said clients, as well as the social alarm caused by this type

of practices.

I. ABOUT THE FACTS GIVING RISE TO THE INITIATION.

Question of penal prejudiciality.

The three complaining parties filed complaints with the Bodies

and State Security Forces in relation to the same facts that were

are dealing with in this proceeding. It is essential to verify if the

complaints have advanced reaching the headquarters of judicial investigation, which supposes

It would be possible to continue the administrative process until the final result is known.

end of criminal proceedings, as established in art. 77.4 of the LPACAP.

FIRST. Of the customer identification operations:

The security measures are the result of a thorough and continuous process.

so of study that encompasses multiple disciplines and areas of knowledge (among

others, legal advice, security, fraud prevention) that has been taken

carried out from the outset with all the guarantees and with the maximum respect.

protection and observance of the principles of article 5 of the RGPD.

The central axis of these security measures is constituted by the

applicable depending on the type of management requested by the client.

(…)

that

1.1.- The technical and organizational measures implemented are appropriate

based on the characteristics of each of the types

management affected by fraud:

The steps used by impersonators to perpetrate fraud

There are basically two types of SIM Swapping requests: duplicate requests

SIM card and requests for change of ownership.

1.1.1.- Guarantees of the duplicate request procedure

of SIM card (...):

(...).

1.1.2.- Guarantees that cover the procedure of change of owner in the

(...):

(...).

1.2.- The technical and organizational measures implemented are reviewed and

continuously updated in accordance with the principle of privacy

from layout and default:

 Measures adopted in the short term

(...).

 Measures adopted in the long term

~

During 2020 TME has worked on the development (…).

~

Additionally and for the year 2021 (…).

1.3.- Clarifications on the operation of Card duplicates:

It's not true that:

(...).

SECOND. The circumstances that have made it possible to overcome

third parties of the implemented security policies and the conse- quence

account impersonation of identity of claimants one, two and three su-

pertain to TME's sphere of responsibility.

(…)

The commercial agents of

have been deceived and induced to commit

human errors when applying the identification operation designed and

required by TME.

2.1.- Non-compliance with the operation by the employees of

distributors and other suppliers:

They provide the contracts signed by THADER, CATPHONE and (...

2.2.- Of the due diligence shown by TME when complying

plir the Identification operation:

Demonstrated at all times, further increasing its efforts from

that is aware of the existence of this type of fraud. insist on the

large amount of (...) in the sense of sending the details of the operation of

identification to all channels.

He has developed numerous actions of (...). In this sense, in order to

reinforce compliance with the operation designed by Movistar, the protocol in-

includes (...) and of (...).

2.3.- Of the continuous innovation of fraud techniques and the sophistication-

tion of the supplanters at the time of perpetrating and evolving this type

of fraud:

It should be borne in mind that these commercials face the (...), it is worth

of them to process a particular management in accordance with the established procedures.

established for this in TME.

2.4.- Of the concurrence of other banking operations not known by

TME necessary to perpetrate bank fraud:

The obligations of authentication and access of third parties imposed by the Di-

Directive PSD2 are not applicable to TME and, furthermore, they did not come into force.

gor until September 14, 2019. Consequently, TME is not responsible

saber of phishing results.

THIRD. The implemented security measures have been demonstrated

adequate, timely and effective in response to the volume of contracting

and the obligations imposed by the applicable sector regulations for

ensure the connectivity of its clients quickly and sustainably in

time.

3.1.- Adequacy, timeliness and effectiveness of security measures

implanted by TME:

The AEPD has only identified three cases of bank fraud (parts relating to

crying one, two and three).

Fraudulent applications identified by TME are minimal and complete.

exceptional if we compare them with the volume of operations of

this type managed by TME.

 Percentage of fraudulent requests detected in card duplicates:

It is X,XXXX%. The imposition of restrictions would imply a rigidity and

an excessive load that could ultimately put at risk:

 Customer connectivity quickly and sustainably

over time in accordance with the sectoral regulations that impose

operators a standard of quality and level of service demanded

tes in order to ensure connectivity.

 Compliance with other principles enshrined in the GDPR,

as the data minimization principle.

On the other hand, the overall percentage of fraudulent applications from

that impersonators use to commit bank fraud (...).

3.2.- Effectiveness of certain processes indicated by the agency:

3.2.1.- The effectiveness of the "victim of fraud" check

There is no such procedure as such.

• Restriction for theft:

Consisting of (…).

• Actions carried out by the fraud department:

Possible fraud detected, (...).

3.2.2.- The effectiveness of the (…).

There is no (...).

3.2.3.- The effectiveness (...)

Among its obligations as a service provider

of electronic communications includes the need to earn

guarantee accessibility to its customer service.

The (...) responds to the set of exposed obligations and, in

attention to these, considers that it is not possible to doubt their

effectiveness.

II. ON THE FOUNDATIONS OF LAW.

FIRST. Regarding the alleged infractions committed by TME:

violation of the principle of typicity.

1.1.- Regarding the conduct of TME: in no case could it be considered

subsumable in any of the precepts that are considered violated

The conduct carried out is not subsumable in any of the precepts whose in-

fraction is imputed, for this it would be necessary that:

- Appropriate technical and organizational measures were not applied

to guarantee a level of security appropriate to the risk.

~

In general, “adequate security” was not guaranteed in the treatment of

lying of personal data.

~

Not being able to demonstrate all of the above.

 Regarding the alleged infringement of articles 5.1 f) and 32 of the RGPD:

TME has appropriate technical and organizational measures

you give:

 Result of a thorough and continuous process of study

that encompasses multiple disciplines and areas of knowledge

legal advice, security, fraud prevention) that are reviewed

and update when necessary.

 In relation to the risk assessment, it should be taken into account

Note that the issuance of a duplicate card may result in

necessary for a client to continue enjoying their service

mobile communications in accordance with article 47 of the Law

9/2014, of May 9 (LGTEL) and Royal Decree 899/2009, of

May 22nd.

 Regarding the alleged infringement of article 5.2 RGPD:

The standard requires demonstrating compliance with the implementation of

appropriate security measures, not its infallibility. infallibility that

it does seem to be demanding from TME, considering only the result

occurred in the case of three claimants, and thus assuming

the existence of strict liability.

 About the alleged infringement of article 25 RGPD:

TME is being accused of violating an article that protects the

privacy in a double aspect: privacy from the design and by de-

effect, without even referring to its full scope in the Initial Agreement.

cio.

 On the definition of the alleged conduct in other sanctioning procedures

tion proceedings filed against TME and Telefónica de España, S.A.U.

The Agency's action is arbitrary because in other files

administrative tests the classification of the conduct has been different (PS/

00114/2019; PS/00453/2019; PS/00235/2020). In all of them

defined the conduct as contrary to article 6.1 RGPD.

With this procedure, the AEPD promotes a proscribed legal uncertainty

and hinders an adequate defense of MSDs, consequently violating

cia the provisions of article 9.3 CE.

1.2.- On the wording of the regulations that are applicable: con-

indeterminate legal concepts that contribute to increasing the uncertainty

legal security and defenselessness of TME:

It invokes several sentences: STS of June 26, 2001 (RJ 2001, 5740); STC

104/2009, of May 4 (RTC 2009, 104); and the STC 145/2013 of July 11

(RTC 2013\145).

The Agency collaborates with this indeterminacy of concepts by referring to

reference to a supposed “principle of data security” of now new form.

emulation on several occasions mentioned, but not included in the RGPD.

1.3.- Subsidiarily: on the interpretation and application of the regulation-

tive made by the agency. Risk of violation of the principle “non

bin in idem” and specialty:

The (...) requires priority in the application of the specific precept on the ge-

general. Therefore, neither Article 5.1 f) nor Article 5.1 f) would be applicable in this case.

5.2 of the RGPD, whose wording is generic and the application of the article proceeds

32 of the GDPR. This specialty is also included in the LO-

PDGDD, which in its article 73 f), unlike article 72.1 a), provides as

serious infraction "f) The (...) that are appropriate to guarantee a level

of security appropriate to the risk of the treatment, in the terms required by

(…)”.

SECOND. TME's conduct is not unlawful.

TME's customer identification operations include technical measures

and organizational measures designed to ensure adequate security of data

personal data of its clients, including protection against unauthorized treatment

authorized or illegal. The rule (…).

The security measures implemented by TME have been demonstrated (...) by

volume of contracting and other procedures, and (...).

In relation to the (...), said contracts respond to the commercial reality and

include all those forecasts that are necessary in order to gain

guarantee its compliance.

THIRD. Absence of guilt.

There is no subjective element of guilt required for the imposition of sanctions.

administrative tions.

TME reveals an unequivocal will to proceed according to Law without

exist in any way intentionality to infringe the norm and having in all

case willingness to comply.

It invokes the STS of December 16, 2015. The conducts in no case are

attributable to TME.

3.1.- The diligent action, in good faith and legitimate expectations of TME:

It has acted with all due diligence when implementing measures

technical and organizational measures (according to the state of the art, the costs of

application, and the nature, scope, context and purposes of the treatment,

the probability and severity of the risks) that are appropriate to gain

ensure adequate security.

As a telecommunications operator and provider of communications services

electronic tions has the obligation to provide said services in a

continuously and in compliance with the obligations derived from the regulations that

application release.

Invokes the follow-up of the "Ex officio inspection plan on contracting

distance in telecommunications operators and energy marketers

gía" and participation in the GT.

He claims to have acted in accordance with the principle of legitimate expectations and invokes the

STS no. 64/2017 of May 22.

3.2.- Exceptional circumstances and beyond TME:

 Failure to comply with the operations established by TME: responsibility

of employees of distributors and suppliers

The AEPD is demanding a (...) simply based on the result

ted, without taking into account that (...) of the distributors, which in his case

they would be breaching the operations. Invokes the STS 1468/2017 of 28

September.

 Possible negligence in the care of personal data by the

users:

TME informs its clients within the framework of their contractual relationship,

Next:

Conditions of Movistar Internet: “Use and custody. The CLIENT

undertakes to make a (…)”.

Specific conditions of the Mi Movistar mobile application: “2.7. Mo-

Vistar will not be held responsible for the loss, theft and/or unauthorized use

authorized by third parties of your credentials or the SIM card of your line(s).

nea/s linked/s, so (...). The same way, (…). Movistar not

is responsible for the use that third parties may make of Mi Movistar

on your device”.

It invokes three Judgments: from the Provincial Court (AP) of Seville, from

May 26, 2014; of the AP of Las Palmas de Gran Canaria, of 20

December 2012; and from the AP of Valladolid on March 10.

 Probable liability of third parties unrelated to TME, such as entities

banking:

Corresponds to the bank (or other providers of the applications

mentioned), (...), to establish the measures that correspond to

ponder, in accordance with the provisions of the regulations resulting from

application to banking entities; and decide on the suitability of

use certain mechanisms to authorize and finalize the transaction.

bank transfer (in this case the SMS).

It refers to the SAP of Alicante no. 107/2018, of March 12 (AC

2018\818).

 Intentional actions of third parties to commit a crime

As the Agency itself indicates, these are "fraudulent practices"

carried out by third parties, of which TME is one more victim.

On the other hand, we must also refer at this point to the en-

previous win by the impersonator to TME commercials

to carry out certain tasks.

It could even be considered that we are faced with a supposed

of force majeure, due to the circumstances described in said

concept, which determines the lack of responsibility or guilt

in the offending behavior.

We are faced with the responsibility of the employees of the dis-

TME contributors and suppliers that have failed to comply with the operations

established, despite the more than evident and proven diligence

TME within the framework of said contractual relationship.

Identity theft can be caused by many factors

outside the will and ability to act of TME, such as

that:

i).- There are third parties who have the will to commit a crime, action

which is inevitable for Telefónica.

ii).- The data that allows identity theft is not ob-

had MSDs. Impersonators must have in their possession

other data (specifically the banks with which these persons operate)

sonas and online banking access credentials) since the

access to SMS messages alone does not allow execution

of banking operations.

iii).- The banking entities are responsible for determining

the necessary security measures to guarantee the consent

ment of the account holder before any banking operation, and

proof of your identity.

Therefore, it is of extraordinary interest to reiterate that there is no link

causal by action or omission, between TME and the final result, due to the

intervention of third parties with sufficient entity to alter it.

FOURTH. Failure to comply with the principle of proportionality.

In the hypothetical case that the AEPD, lacking adequate legal support and

with the sole purpose of imposing a fine, considers suitable and indispen-

able to financially sanction TME, the amount of such sanction must

be estimated according in all cases to the principle of proportionality.

Invokes the STS of June 2, 2003 and Considering 4, 129 and 148 and ar-

article 83 of the RGPD.

The economic sanction that would correspond is totally ineffective and wasteful.

provided. Nope

consideration the provisions of the articles

have been had in

83.1 and 83.2 of the RGPD.

4.1.- Of the appreciated aggravating factors:

1. Seriousness of the offense

It refers to the Judgment of the National High Court (SAN) 00496/2017,

in which the evaluation of the

conduct as serious by the SESIAD, to the extent that it does not

non-compliance was found to be widespread.

In

Consequently, it cannot be considered

fraction is serious.

that the nature of the

2. Duration of the events.

The duration of the allegedly irregular treatment could not exceed

der of the moment when SIM card duplication was perfected

of the three claimants.

It is surprising that the Agency appreciates the aggravation of lasting

tion, understanding that the facts cover a period of more than a year, and

At the same time, the lack of continuity is considered as a mitigating factor.

number of the infraction.

3. Number of stakeholders affected

Lack of due congruence in relation between the illegal act committed and the

proposed sanction -only 3 cases-.

4. Level of damages suffered

In no way can TME be attributed responsibility for the ma-

materialization of bank fraud, since your responsibility ends

with the result of the duplicate card, but is not responsible for

the customer identification policies established by the entities

banking.

The assessment of the aggravating circumstance contemplated in article 83.2.a) does not

can be based on the perpetration of this type of crime.

5. Intent or negligence

The

events that occurred with the three claimants cannot be considered

-

considered as a representative sample of the level of commitment

demonstrated by TME and, much less, of the degree of efficacy reviewed

have security policies that are designed to cater to

a volume of customers that exceeds 8 million.

6. Responsibility of the person in charge

It seems that the AEPD mixes in its argument the banking entities

disputes with distributors.

7. Category of personal data affected

TME processes only identification data (Name, surnames, DNI).

In this sense, it is evident that the category of data affected

by fraud, not only do they not fall into the category of sensitive data re-

caught in art. 9 of the RGPD, if not that the AEPD itself classifies them

as "low risk data", according to the category of personal data.

made in section 6.2.3 of the “Guide for the management and notification

tion of security breaches.

4.2.- Of the appraised mitigating factors:

The Agency has not taken into account certain circumstances that result

in the application of said mitigating factors. On the other hand, you forgot to include in

that list of mitigating factors, others that also apply and that are fundamental

mental.

In relation to the circumstances not taken into account:

In relation to article 83.2.c) RGPD. Measures taken by the res-

responsible for mitigating the damages suffered by the interested parties.

two: the AEPD does not refer to (...).

In relation to article 83.2.f) RGPD. Degree of cooperation with the

control authority: the AEPD does not refer to the collaboration

carried out by this party within the WG.

In relation to article 76.2.a) LOPDGDD. The continuing character of

infringement: the AEPD does not take into account the tiny percentage that

n the cases of fraudulent SIM duplication requests in relation to

with the volume of transactions managed by TME, which barely exceeds

0%.

This party understands that the mitigating factor contemplated in article 76.2.d) re-

It is decisive for the purposes of assessing a possible economic sanction.

The identity thefts produced in the cases of the three claims

maintenance would not have been possible if the supplanter had not performed

a previous illegitimate capture of the personal data of said clients.

(The underlining, italics and bold are from TME).

These allegations have already been answered in the Proposed Resolution and are reiterated,

in part, in the FD of this Resolution.

SIXTEENTH: After the period of arguments granted in the Agreement of

initiation and presented allegations, dated May 4, 2021, by the instructor

of the procedure, it is agreed to open a trial period in the following

terms:

"1.

The international claims are considered reproduced for evidentiary purposes.

put by A.A.A., C.C.C., D.D.D. and its documentation. Also the documents

documents obtained and generated by the Inspection Services before TELEPHONE

NICA MÓVILES ESPAÑA, S.A.U, and the Report on previous actions of the

Subdirectorate General for Inspection of Data that are part of the file

you E/11418/2019.

two.

Likewise, they are considered reproduced for evidentiary purposes, the allegations

tions to the initiation agreement PS/00021/2021 presented by TELEFÓNICA MÓ-

VILES ESPAÑA, S.A.U, on March 8, 2021 through the Registry

General of this Agency, and the documentation that accompanies them:

(...).

3. Practice with today's date, a requirement to: A.A.A., C.C.C. and D.D.D., to

in order to provide within 10 business days, information on the course of the

of the complaints filed for these events, as well as information on

the criminal proceedings that are pending in his case."

SEVENTEENTH

: In response to this last request:

On May 25, 2021, the claimant one provides a certificate from the Court

of Instruction 2 of ***LOCALIDAD.3, in which the Proceedings procedure is followed

Previous No. XXXXX for fraud, in which she appears in a damaged condition.

On May 7, 2021, the claimant two states that they are not aware of

ment of any data about the possible investigations that may have been given to

from the complaint filed.

On May 21, 2021, claimant three states that on the past 11

February 2021, declared in the Court of 1st Instance and Instruction No. 01 of Maja-

dahonda in the procedure of Preliminary Proceedings XXXXX in his condition of prejudice

accused/offended, in which he appears as investigated F.F.F. He adds that he expanded the complaint

Initial evidence presented to the Civil Guard on September 28, 2020. Provides

an mp3 file, provided by the Municipal Office of Consumers, which includes

the recording of the change of ownership of the service in favor of the latter.

EIGHTEENTH: On July 21, 2021, the Investigating Court is requested to

tion no. 2 of ***LOCALIDAD.3, by email, information on the procedure

Preliminary Proceedings No. XXXXX, and on the criteria of the respective judicial body.

to the concurrence of identity of subject, fact and basis between the presumed in-

administrative fraction and the criminal infraction that could correspond, to proceed,

where appropriate, to the immediate suspension of the procedure initiated, by virtue of the

ceptuated in article 22 of the LPACAP.

NINETEENTH

: On July 28, 2021, an email is received from the

Court of Instruction no. 2 of ***LOCALIDAD.3, in which the judge reports the following-

following:

“Regarding the requested petition, I inform you that the complaint filed by

Mr. A.A.A. was not filed against the company (sic) TELEFONICA MOVI-

LES ESPAÑA SAU despite the fact that in the complaint it was reported that a duplicate was made

of your card (sic) SIM no. ***PHONE.2 and he had not requested it. In

this sense and in response to the request there is, for this reason, no identity

of subjects that leads to the suspension of the procedure."

TWENTIETH: On September 16, 2021, the instructor of the formal procedure

mula Proposal for a Resolution, in which it proposes that the director of the AEPD

sanction TELEFÓNICA MÓVILES ESPAÑA, S.A.U., with CIF A78923125, for in-

fraction of article 5.1.f) of the RGPD, typified in article 83.5.a) of the RGPD and in the

Article 72.1.a) of the LOPDGDD, with an administrative fine of 1,000,000'00 (one mi-

million euros).

On September 20, 2021, through the Electronic Notification Service

cas and Enabled Electronic Address, the Resolution Proposal is notified.

TWENTY-FIRST: On September 22, 2021, TME requests the extension

nation of the term to formulate allegations to the Resolution Proposal.

TWENTY-SECOND: On September 23, 2021, the Agency grants the

requested expansion.

TWENTY-THIRD: On October 11, 2021, TME makes allegations to

the Resolution Proposal in which it is reiterated in each and every one of the allegations-

tions made to the Initiation Agreement (antecedent FIFTEENTH) and adds others:

PREVIOUS: ON THE INITIATION OF THE PUNISHING PROCEEDINGS.

The AEPD was carrying out an independent investigation which, at least

us the Operators that participated in the GT, and specifically, TME, were not

was up to date.

Indeed, the applicable regulations establish that the supervisory authority

will have a series of powers, for which purposes it grants up to 22 types of

functions and up to 10 corrective powers, but all of them must be exercised si-

following the principles of the legal system, and in that sense, the claim

sion to be using any of those other tools provided for in the law,

when in reality what he was doing was investigating to settle the responsibility

operators and penalize them with unprecedented economic fines.

can not be interpreted in any other way than as a lack of transparency.

cy and discretion.

The accusations made by the AEPD turn TME into a sort of co-

operator necessary for the achievement of this type of fraud, when in

reality is another victim of fraudsters.

The guarantee of a zero fraud result is not required in view of the

principles established in the RGPD, nor of the corresponding obligations

to the Data Controller.

I. ABOUT THE FACTS GIVING RISE TO THE INITIATION.

It was requested that the procedure be suspended and the AEPD has limited itself to

indicate that such procedures are not directed against TME, referring to

that there is no identity of the subject to dismiss the allegation of prejudicial

criminality.

It has ignored the content of the investigations that have been carried out

now, which is relevant to determine if what was being treated in

criminal proceedings are similar or important issues for

this procedure, in such a way that it could not continue until knowing the

final outcome of the criminal proceeding.

It invokes Judgments no. 2249/2016 and no. 1907/2017 of the Chamber of the

Tencioso-Administrativo of the Supreme Court dated October 18,

2016 and December 5, 2017, respectively and argues that there is prejudice

criminal jurisdiction when "the decision to be issued in the criminal process conditions

the judgment of the contentious-administrative appeal, so that

the latter can be pronounced without knowing the result of the former", which is precisely

exactly what could happen in this case as both procedures are one

extension of each other.

And, although there is no identity of subjects, the results of the actions of in-

investigation of criminal proceedings directly affect the procedure

sanctioning, not only to determine what really happened at the time of co-

to get involved in fraud, but also in the event that it was finally imposed

a penalty, determine the appropriate amount.

For this reason, it is requested that the different Courts be directly required to

so that they provide the status of the complaints filed, as well as the

content of criminal proceedings, in order to agree on the suspension

of this procedure by penal prejudiciality.

FIRST. OF THE CONDITION OF TME AS RESPONSIBLE FOR THE TRA-

PROCESSING AND DELIMITATION OF PROCESSING OPERATIONS

PURPOSE OF THE PUNISHMENT PROCEDURE.

At no time has the AEPD defined which operations or activities

of data processing is specifically referring, sending-

to this with a general character and in an absolutely arbitrary and particular manner.

far

It does not identify which are the processes or activities that are the responsibility of TME,

in such a way that they can be separated from those who fall within the scope of res-

responsibility of third parties (banks).

It is necessary to clarify that the treatment processes or activities that are

they question are none other than the processing of identifying data

(name, surnames, DNI), in order to identify the client as a step

prior to the management of a specific request (in this case two requests

specific, the duplication of SIM card and the change of ownership), being the

legitimizing basis of said treatment is the execution of the existing contract.

between TME and its client. That is, data processing operations

would consist of contrasting the information provided by the request

appointment with the information contained in our systems.

Refers to Guidelines 07/2020 of the European Committee for Data Protection

(CEPD), specifically: “(…) In practice, this may mean that the

control exercised by a particular entity may extend to the entire

ity of the processing in question, but may also be limited

to a particular stage of the processing” and the Judgment of the CJEU of 29

July 2019: “(…) On the contrary, [...] that natural or legal person does not

can be considered responsible for the treatment, in the sense of said

disposition, in the context of operations that precede or are subsequent to

in the general chain of treatment for which that person does not

ends the ends or the means.

It considers that the Agency erroneously links TME with a series of operations

rations or treatment activities that should be left out of the object

of the procedure. The Agency attempts to hold it responsible for operations

or treatment activities carried out by third parties, although certainly linked to

linked to other treatment operations that are the responsibility of

TME. TME cannot be held responsible for the fact that a certain

type of bank fraud because, if this were so, it could be res-

responsible for all illegitimate access that occurred within the framework of the

provision of services of any company that verified the identity

of your customers via mobile phone.

What the Agency questions is not compliance with the GDPR principles

or the diligence of TME when executing the duplicate card. What I know

has called into question is whether the identification policies that TME

has implemented are robust enough to prove

that the applicant of a certain management is who he claims to be.

TME is the first party interested in having said identification process carried out

without cracks and with the greatest possible guarantees and has implemented me-

adequate security measures in attention to the risks derived from the activity

treatment life for which it is responsible.

SECOND. ON THE ADOPTION OF TECHNICAL AND ORGANIZATIONAL MEASURES

YOU GO APPROPRIATE.

2.1

TECHNICAL AND ORGANIZATIONAL MEASURES IMPLEMENTED

Attached as Annex 1 is the document "(...)", which contains the latest version of the

document that (...). The central axis of these measures is constituted by the

(...) that is applicable depending on the type of management requested by the client.

tea.

Regarding (…):

It is done exclusively through (…). TME has adopted the measure of

most effective security and the one that offers the most guarantees in terms of identifying

care for a client, which is none other than verifying in person that some

who is who he says he is. The Agency has not clarified at any time

what sense does it consider that said operation is contrary to the Regulation or

nor does it mention what elements of the identification policy would have to be

have adapted.

The measures are not only adapted to the standards that have been applied

the main players in the telecommunications sector, but

in certain respects they surpass them. It has already been shown that the system

identity validation method that is contemplated in the "(...)" has the

same guarantees as the strong authentication system established

by Directive 2015/2366. The Agency has not analyzed in any way

arranged by TME in its operations, whether or not they are co

measures

lie yes

-

inherited with PSD2.

It has already been shown that the “(…)” is aligned with the recommendations

established by the Agency itself in the report "Inspection plan of offices

cio on distance contracting in telecommunications operators

and energy marketers”, the AEPD has not ruled on

its Motion for a Resolution in this regard.

Regarding (…):

The (...) obliges the agents of (...).

In addition, currently this type of management is derived and processed by a

(...). The way in which it manages the (...) attached as Annex 2. In short,

(...). As stated in its report "Ex officio inspection plan (...)",

this way of identifying customers can be considered a standard within

companies in the telecommunications sector.

of

TME disagrees with one of the Agency's statements, in con-

decree, contained on page 93 of the proposal, argues that:

1.- TME does not allow you to request or manage a change of SIM card in the

(...), it is only possible to request it in person at the store.

2.- The (...) are equivalent. Now, even being equivalent, it is evident

that they cannot in any case be the same. TME cannot adopt

the technical and organizational measures related to the processing of

cation without taking into account the channel, the type of management for which

izes the treatment, and the fulfillment of the obligations that it has as

operator.

3.- In no case has it been said that it is possible to obtain a duplicate of

SIM card without going in person to a store. It is not what has

happened in the cases of CLAIMANTS ONE, TWO and THREE.

2.2 REVIEW AND UPDATING OF TECHNICAL AND ORGANIZATIONAL MEASURES

IMPLEMENTED NIZATIVES

TME has amply proven that it has carried out revision efforts

sion and reinforcement of operations.

Efforts have been channeled along three axes:

a) Reinforcement of existing operations:

•(…). Attach as Annex 3 the document "(...)" containing:

-. Excerpts from publications made in the (...), between the years 2019 to

2021.

.- Excerpts from news published in (...) of which they are also part

the (...) between 2020 and 2021.

.- Implementation in October 2020 of the new (...) (Annex 2). (…)

(Annex 4).

b) Implementation of long-term transversal projects:

TME has worked on the development of (...).

c) Share the problem with this Agency and other interested parties.

sad:

.- In order to study possible ways of improvement without having received from

the AEPD, not a single proposal of those additional measures that could

would seem to be overlooking.

.- You have dealt with this problem with (...)", with the aim of knowing and

adapt, where appropriate, effective measures that contribute to reducing this

type of fraud (Annex 5 "(…)").

.- You have created a (...) whose first meeting took place in the month of

September 2021. (…).

It cannot be said that he has not carried out a task of constant adaptation

depending on the new risks identified.

2.3 ASSESSMENT OF THE ADEQUACY, TIMELINESS AND EFFECTIVENESS OF

THE TECHNICAL AND ORGANIZATIONAL MEASURES IMPLEMENTED

He alludes to the FD Quinto and that the AEPD has not stopped at any time to

assess these aspects, few efforts have been dedicated to the analysis of the

proportionality in relation to:

Technical knowledge: TME was unaware of the authorization obligations

Tentication and third-party access imposed by the PSD2 Directive. Said obli-

regulations do not apply to it and did not enter into force until 14

September 2019.

Implementation costs: they are very high and so is the implementation time.

tion that entails the implementation of far-reaching measures.

Nature, scope and purposes: to verify the identity of clients in

a company dedicated to providing communications services

electronic and, as such, has the obligation to provide said services of

continuously and in compliance with the obligations derived from the regulations

which results from application.

In the Rationale the Agency only mentions a couple of the measures of

security implemented by TME. It has not even been entered to do an analysis

specific system of the adequacy, timeliness and effectiveness of all measures

that you have implanted.

TME has certified and duly audited the processes and operations

You are going to be questioned in this file. Specifically, the suitability and

Ensuring policies for verifying the identity of clients, is

object of analysis of the UNE 19601 standard for Com-

Criminal compliance. In particular, control C.047, relating to the "Contracting

Client identity verification", is specifically aimed at contrasting

the adequacy of the operations, the way to verify the identity of the clients

and the existence of monitoring and control mechanisms.

To guarantee compliance with this Criminal Compliance regulation, it is

necessary:

-. Obtaining the "Personal Compliance Management System Certificate"

nal" (hereinafter, SGCP). This certificate is renewed every 3 years and is

subject to the results of the periodic follow-up audits carried out.

They provide:

As Annex 6.1 and Annex 6.2, the documents "Certification 2017 AE-

NOR 19601" and "2020 AENOR 19601 Certification", which accredit the certification

certification of TME in compliance with this regulation since the year

2017.

As Annex 7.1, the document "Certification 2020 EQA 19601", which

accredits the certification of TELEINFORMATICS AND COMMUNICATIONS,

S.A.U. (TELYCO) in compliance with this regulation since the year

2020.

-. Carrying out periodic follow-up audits. They contribute the two

Documents:

“Audit 2021 AENOR 19601” (Annex 6.3) and “Audit 2021 EQA

19601” (Annex 7.2). In both, compliance with the control is verified.

C.047. Specifically, the result of this audit process de-

shows that TME has:

1.- OPERATIONS.

2.- VERIFICATION OF IDENTITY AND ASSOCIATE DOCUMENTATION-

GIVES.

3.- MONITORING and CONTROL.

The Crime Prevention Model used by TME has also been audited.

done by the consultant (...) through its Internal Control Report on the

Organization and Management Model for Crime Prevention. It provides the

says, the purpose, scope and conclusions of said Report in the document

to “2020 EY Internal Control Report Crime Prevention Model”, as

Annex 8.1 and the document "Annex I Report 2020 Controls analyzed EY"

as Annex 8.2.

On the other hand, it does not consider that an analysis of the

adequacy of the measures if their effectiveness in terms of

No. of volume of transactions affected:

The Agency insists that we are dealing with a fundamental right protected

governed by the CE. But, it is no less true that, as indicated by the RGPD "the

The right to the protection of personal data is not an absolute right.

mourning, but must be considered in relation to their role in society and

maintain a balance with other fundamental rights, in accordance with the principle

principle of proportionality."

Lastly, it is not admissible for the Agency to allude in its Resolution Proposal

tion to an alleged violation of a policy that is not applicable to TME

(Know Your Costumer (KNY)).

THIRD. OF THE RESPONSIBILITY OF TME IN CASES OF SU-

PLANTATION OF IDENTITY OF THE THREE CLAIMANTS

3.1 RESPONSIBILITY OF THE DATA PROCESSOR

TME entrusts part of the data processing operations subject to

this procedure to trusted suppliers. The providers selected

tioned go through a rigorous selection and hiring process that

contemplates the application of specific security measures, depending on the

type of contracted provider. Provides as Annex 9 and Annex 10 the (...).

Both documents are intended, respectively:

-. (...).

-. (...).

Ultimately, the application of the aforementioned internal regulations has

As a result, the imposition of the security measures that are included in

on (...), attached as Annex 11.

He refers to what the AEPD affirmed on page 92 and argues that in no way

moment has tried to evade the responsibilities that correspond to it

respect to the safety of the treatment, but to show the compliance

compliance by TME with the obligations that the protection regulations

tion of data imposes on the person in charge, in terms of:

-. Have duly regularized the relations of contract of trade

treatment with the affected suppliers in accordance with the provisions

placed in article 28 RGPD.

-. Transfer with due diligence and clearly to those in charge

treatment documents the instructions that govern the treatment operations

commissioned treatment.

Thus, the AEPD considers it proven in the Resolution Proposal that TME has

duly regularizes relations with those in charge of treating

I have indicated that "it has been verified in the alleged allegations the

existence of contractual clauses that refer to “Instructions

tions” documented by TME (…).”

Bearing in mind that the impersonations of the complaining parties

ONE, TWO and THREE have in common the concurrence of punctual errors

of the operation designed by TME, and that the Agency has verified the commission

sion of said non-compliances, understands that it is very important to highlight the

difference between:

That the measures implemented are appropriate.

That the measures have been correctly transferred to those in charge

That the measures have been breached by those in charge.

-

-

two.

-

In other words, it is necessary to differentiate between the measures implemented being sufficient

and that these, even though they are sufficient, could have been breached

tually by those in charge.

He argues that having proven in this proceeding that, if

been for said non-compliances, said substitutions would not have occurred.

tations, considers it essential to define the responsibilities that

assumed by each of the parties in relation to the processing operations.

of disputed data. It refers to the Guidelines 07/2020 where it is said: So-

Both those responsible and those in charge can be fined in case

breach of GDPR obligations that are relevant

for both, and both are directly accountable to the authorities.

from supervision (...).

In relation to this aspect, TME also affirms that according to article

28.10 of the RGPD, the person in charge can be considered as responsible for the

treatment in case of “determining the purposes and means of the treatment”. According to

indicates, the aforementioned Guidelines would clarify that ““Determining the purposes

and the means is equivalent to deciding respectively the "why" and the "how" of the

prosecution"

In short, it is alleged that TME cannot be held responsible

for this breach, since this company would have acted with all diligence

required agency, and that the possible security flaws when the certificates have been issued

duplicates of the SIM cards would be attributable to the supplier, since this

would have failed to comply with his instructions.

3.2 RESPONSIBILITY OF THE BANKING ENTITIES

It seems that the AEPD wants to make TME responsible for the commission of the

bank fraud carried out by the fraudsters in all three cases.

The obligations of authentication and access of third parties imposed by the Di-

Directive PSD2 are not applicable to TME and, furthermore, they did not come into force.

gor until September 14, 2019.

For all these reasons, TME cannot be held responsible for the treatments carried out.

acted by other responsible parties (banking entities), nor can it be attributed to

TME the responsibility to adopt security measures related to

data processing operations carried out for a different purpose.

II. ON THE FOUNDATIONS OF LAW

FIRST. ON THE ALLEGED INFRINGEMENT THAT CONTINUES

BEING COMMITTED BY TME: VIOLATION OF THE

PRINCIPLE OF TYPICITY

It has been proven “that TME has documented policies of

data protection that establishes the way of acting of TME and of

the managers".

1.1 ABOUT THE CONDUCT OF TME: IN NO CASE COULD IT CONSIDER

DERARSE SUBSUMABLE IN ARTICLE 5.1 F) RGPD.

The AEPD has verified that the conduct is not subject to article 5.2

RGPD, that is, it recognizes that TME has complied with the provisions of article

5.1 and has been able to demonstrate it, verifying the application of measures

appropriate technical and organizational measures that guarantee a level of security

that is appropriate to the risk. These measures are reviewed and updated when

it is necessary in order to guarantee the security of the treatment.

The Agency is demanding infallibility from TME, attending only to the

result produced in the case of only three claimants, and assuming

again the existence of strict liability (outlawed in our

legal system) as sufficient justification to consider that there is

an offence, and that it is very serious. It refers to the CIPL (Center for Information

Policy Leadership), who in his comments about the guidelines on the

notification of violations of personal data of the WG of Article 29 (“Com-

ments by the Center for Information Policy Leadership On the Article 29 Wo-

rking Party’s “Guidelines on personal data breach notification under Regula-

tion 2016/679” Adopted on 3 October 2017”), illustrates well the difference between

risk mitigation and infallibility, by indicating that it cannot be an obligation

tion for organizations to ensure absolute security of operations.

purposes of data processing ("It cannot be an obligation for organizations

to guarantee absolute security of data processing activities”).

Likewise, it has not been taken into consideration that even the WG on protection

tion of data of article 29, in the “Guidelines on the notification of the

violations of the security of personal data in accordance with the Rule-

2016/679" recognizes that, even if security measures are implemented,

security, there may be risks, indicating that:

"(…) a key element of any security policy of

data is to be able, to the extent possible, to prevent a breach and,

when, despite everything, it occurs, react quickly".

It also refers to an INCIBE article:

"To reduce the likelihood of these types of incidents occurring

(…)"

"In this way we will avoid, as far as possible, the leaks of

information and the loss of image of our company".

And to the Ruling of the AP of Valladolid (Section 1) no. 74/2010 of March 10-

zo (AC 2010\368), in relation to the alleged breach of security measures

security by a bank, states that:

"In any operating system, even the traditional one, there are

risks and what is decisive for attributing responsibilities will be whether

used, sufficient guarantees were given, without being able to reach the

contrary conclusion by the mere fact that subsequently

security systems have been improved, which is logical

modernize and improve in the face of new fraudulent practices

ries that make the previous ones ineffective".

TME considers that it has been proven that security measures are not

have been violated, but there has been a breach of the operations

established by TME and that actions by third parties have taken place.

us to her

Thus, the legality or not of a security measure (that is, its adequacy)

tion) is determined by its contribution to the reduction of the proba-

probability of occurrence of the incident, and without any doubt, if the probability

occurrence of a fraudulent request for SIM duplication (for

any of its modalities) is X,XXXXX %, it is a percentage

minimum rate.

In relation to the risk assessment, it should be noted that the

issuance of a duplicate SIM card may be necessary for a

customer continue to enjoy their mobile communications service. Namely,

The data processed is identifying the client, in order to prove

the identity of the applicant for the management and to be able to continue providing the service

vice of mobile telephony, in accordance with the requirements of current regulations:

article 47 of the LGTEL, article 3. e) of RD 899/2009, of May 22 and the Or-

in IET/1090/2014.

1.2 ON THE DRAFTING OF THE REGULATION THAT RESULTS FROM APPLICATION

CATION: UNDETERMINED LEGAL CONCEPTS THAT CONTRIBUTE

YEN TO INCREASE THE LEGAL INSECURITY AND DEFENSE OF

TME.

He invokes the Judgment of the Supreme Court of June 26, 2001 (RJ 2001,

5740), which recalls the doctrine of the Constitutional Court.

He alludes to the importance of the regulatory norm not making formulations

vague, open or excessively broad of the offenses and sanctions, which

lack sufficient determination, since “the sanctioning organ would be allowed

tionor to act with excessive discretion and not with the prudent and reasonable that

would allow a proper normative specification” (STC 61/1990, of March 29,

zo).

The AEPD has not taken into account the allegations made by TME, limiting

referring to recitals 7 and 13 of the RGPD, to invoke the right

right to data protection as a fundamental right, and to the definitions

of article 4, among which it recognizes that legal concepts are not included.

to which we made reference in the allegations to the Initial Agreement

cio. For this reason, the ambiguity and indeterminacy of the

concepts included in the precept that this AEPD considers violated,

such as: “adequate security” or “appropriate technical and organizational measures

pious”.

Invokes article 9.3 of the CE, the STC 104/2009, of May 4 and the STC

145/2013, of July 11 and argues that the Agency continues to promote insecurity

legal authority and hindering the defense of TME, which may be violated in con-

sequence certain principles that are guaranteed to constitute

tionally (article 24, 25 and 9.3 of the CE).

1.3 SUBSIDIARILY: ON THE INTERPRETATION AND APPLICATION

OF THE REGULATION MADE BY THIS AGENCY. RISK OF VUL-

NERATION OF THE PRINCIPLE OF SPECIALTY.

In relation to the specialty principle, the Agency limits itself to collecting the

expressed arguments, without reaching a pronouncement on this aspect. In the

Resolution Proposal “redirects the imputation of the initial infractions

cially considered. The legal qualification of the facts that are imputed

is classified as a single infringement derived from the infringement

of article 5.1. f) of the RGPD” without taking into account the principle of specialization.

ity, and specifically article 32 of the RGPD.

A violation of the principle of specialty requires priority in the application

cation of the specific precept over the general. Ultimately, of the items

that were referenced at the time, would also be article 32 of the GDPR.

well regulated in the LOPDGDD, which in its article 73 f), unlike the article

Article 72.1 a), establishes as a serious infraction “f) Failure to adopt those

technical and organizational measures that are appropriate to guarantee

establish a level of security appropriate to the risk of processing, in the terms

required by article 32.1 of Regulation (EU) 2016/679”. So, in

In no case could the conduct of MSD be classified as very serious.

SECOND. ON THE CLASSIFICATION OF THE ALLEGED CONDUCT IN

OTHER SANCTIONING PROCEDURES INITIATED AGAINST TME AND TE-

LEFÓNICA DE ESPAÑA, S.A.U (TDE): ERROR IN THE QUALIFICATION OF

THE INFRINGEMENT.

It should be specified that this part does determine how your

situation, since the Agency's action is arbitrary. In the PS/

00114/2019, PS/00453/2019, PS/00235/2020, the criminalization of the conduct has

been different and the sanction imposed as well. In all of them, the

conduct of TME as contrary to article 6.1 RGPD (“lawfulness of the treatment

to") for allegedly having processed the data of the complainants without

There is a legal basis for it. However, in this case consider the

conduct contrary to article 5.1 f) of the RGPD. Likewise, the penalty

The proposal has also been far from the proposal in the framework of this experiment.

tooth, despite the application of article 83.5 a). It's more than obvious

that with this procedure, the AEPD promotes a proscribed legal uncertainty and

hinders an adequate defense of MSDs, consequently violating the pre-

visions of article 9.3 CE.

THIRD. THE CONDUCT OF TME IS NOT UNLAWFUL

Regarding the illegality of the conduct by the Agency “it is considered that

responds to the type of offender and the title of guilt”, without analyzing the allegations

tions made by this party in this regard.

Insists on rejecting the unlawfulness of the conduct based on the following

arguments:

-. The customer identification operation includes technical measures and

organizational measures designed to ensure adequate security of the

personal data of its clients, including protection against treatment

unauthorized or unlawful lying. He argues that the rule does not require infallibility

of these measures.

-. The measures implemented have proven timely and effective in

attention to the volume of contracting and other procedures, and the obligation

tion of ensuring client connectivity quickly and

sustainable over time. TME's actions have not injured or

endangered any protected legal right, but rather responds to the need

necessary balance between ensuring the security of data processing

personal rights and guarantee the provision of community services.

electronic cations in accordance with the rest of the regulations that result from

app.

-. In relation to the contractual relationship that exists with the distributors

providers and other providers, these contracts respond to the reality

mercantile and include all those provisions that are necessary with the

purpose of ensuring compliance. In this sense, the AEPD yes “has

confirmed that TME has documented protection policies

tion of data (…)”. However, it does not accept the allegations made

for this part in that sense.

QUARTER. NO FAULT

There is no subjective element of guilt required for the imposition of

administrative sanctions. Quite the contrary, since TME's attitude reveals

an unequivocal will to proceed in accordance with the law without actually existing

any intention to violate the norm, and in any case having the will

of compliance.

TME does not question whether or not legal persons have the capacity to infringe

the rules to which they are subjected, but the absence of their guilt, and

consequently, the absence of infraction of the norm.

This lack of guilt is manifested around the fact that:

-. TME's conduct was carried out with all professional diligence

demandable, that he acted in good faith, and that, for that reason, it cannot be imputed

sele a guilty act.

-. The choice and supervision of those in charge of treatment has been determined

performed with all due professional diligence. Also, you must

insist on the own responsibility of the person in charge of the treatment.

-. The behaviors that have provoked the consequences exposed in any

In some cases they are attributable to TME.

4.1 DILIGENT ACTION, GOOD FAITH AND LEGITIMATE TRUST

OF MSD

In relation to the diligence of TME, it is striking that in the Proposal

of Resolution, on the one hand, certain affirmations are indicated that include va-

positive lotions and on the other hand, in contrast to indicate other ne-

gatives.

In relation to these arguments, it is appropriate to make a series of clarifications.

First of all, it should be noted that TME is not specifically dedicated to the

management of personal data, but it is a company dedicated to the provision

tion of electronic communications services.

TME has not limited itself to invoking the absence of guilt, but rather everything ex-

put into the allegations made is fully demonstrative of the rigor and

diligence with which he has acted.

The AEPD maintains in the Resolution Proposal that "the infraction becomes

not because of the lack of a specific security policy for the expedition

of SIM duplicates, but because of the need for their review and reinforcement (...)

It is not enough to have a security policy, but to adapt it to

mitigate risks. (…)". However, it has been proven that TME treats

constantly decreases in the improvement of the measures available to him with the

objective of avoiding identity theft in the different processes of

contracting and procedures that are requested, in the training and in the adaptation

security protocols within the organization. That is to say, it has remained-

fully proven that TME implements control measures

adequate, which are reviewed and reinforced. Invokes the UNE certification

19601 of Criminal Compliance Management Systems, as well as having due

audited its Model of Organization and Management for the Prevention

of Crimes including control C.047 related to the "Verification Hiring

cation client identity".

However, the Agency continues to focus only on the result produced.

acid, disregarding the circumstances completely unrelated to TME that

have taken place, thus demanding strict liability.

The AEPD has recognized that TME has contractual clauses that make

cen reference to documented instructions, in addition, as a provider of

electronic communications services, has the obligation to provide it in

continuously and at all times has acted in good faith and in a pro-

active and diligent (including participation in the GT). Summon the STS of 17

of December 1988 that says: "it is not fair to sanction those who act in

good faith proceeding to leave the sanction without effect when the act of the accused

sin was due to a certain belief that excludes guilt.

4.2 DUE DILIGENCE IN THE CHOICE AND SUPERVISION OF THE

CHARGED OF THE TREATMENT AND RESPONSIBILITY OF THIS:

In the Proposal for a Resolution it is stated that “The ultimate responsibility is

about the treatment continues to be attributed to the person in charge, who is the one who determines

undermines the existence of the treatment and its purpose”, and again mentions the

subject to article 5 of the RGPD

There is a breach of the operations established by TME: liability

ity of those in charge of treating MSDs and certain actions

of third parties outside the sphere of action and responsibility of TME.

It invokes that the Agency has recognized the existence of contractual clauses

that refer to documented instructions, therefore, you acknowledge

diligent action, however, dismisses the allegation made to the pointer

lar that “the treatments carried out by those in charge will be made on behalf

of the person in charge, that is, TME”.

He invokes articles 1902 and 1903 of the Civil Code and insists that his conduct

has been diligent, since, for example:

- The selected suppliers go through a rigorous process of

selection and hiring that contemplates the application of measures

specific security measures, depending on the type of contracted provider.

do.

- It has a consolidated and adequate procedure for verifying

tion of the identity of the clients, and with instructions duly

documented to their data processors.

- In the contracts with those in charge, certain

undermined disciplinary and penal measures, and, for the purposes

to guarantee compliance with the identification operation in

store, a penalty has been established for the entire face-to-face channel

additional payment for each procedure carried out and documented incorrectly.

mind by a commercial. It entails the implementation of

a monthly certification process of the compliance of the distributors

buidores.

- Certification of the UNE 19601 Systems of

Management of Criminal Compliance and compliance, both by

TME as well as the rest of the group companies, from control C.047

relating to the "Contracting Customer Identity Verification". Namely,

The existence of “(…)” is credited, among other things.

- The (...) is being carried out.

- The “(…)” has been included for authorized users.

Refers to the STS 1232/2018 of July 18, 2018 and the STSJ of Madrid

568/2020 of September 10, 2020. In short, in no case was the

the duties of vigilance that weigh on TME in relation to the persons

nas acting on their behalf.

The Agency has not taken into account the content of article 28.10 of the RGPD.

Therefore, what happened was not due to vulnerabilities in the procedures.

established procedures, nor in the instructions given to those in charge of processing

treatment, but to the non-compliance of the operation designed by the

commercial agents of the channels for the attention of the requests of the

different procedures referred to in this file, and consequently

non-compliance with the instructions given by TME by the employers.

employees of said managers.

He insists that, from the foregoing, it can be concluded that the AEPD is demanding

strict liability, based simply on the result, without

bear in mind that TME has acted with complete diligence in the relationship

with their treatment managers. Adduces the STS (Litigation Chamber-

Administrative, Section 3) no. 1468/2017 of September 28 (RJ 2017\4422).

It is necessary, therefore, to verify guilty intervention on the part of the

of TME, which has not occurred in this case, without there being either “fault in vi-

gilando”. As long as this element is not complied with, sanctions cannot be imposed.

tion and the sanctioning procedure should be archived.

4.3 EXCEPTIONAL CIRCUMSTANCES AND OUTSIDE TELEFÓNICA:

• Possible negligence in the care of personal data on the part of

users: the users themselves have the responsibility of custodian

properly disclose your personal data.

By using the Internet, they can share certain information

personal, which may imply that it is used by third parties for illicit purposes.

cough. This is outside the scope and capacity of action of TME, since

that the data that sometimes allows identity theft can

be obtained from the information that, if applicable, may have been disclosed by the

user at any time, or from a lack of duty of care when guarding

your passwords or personal information.

It refers to the AEPD Guide “Data protection and crime prevention” and

recommendations on Phishing. These circumstances have not been

taken into account by the Agency.

Likewise, TME informs its clients within the framework of their contractual relationship

a series of clauses that require diligence regarding access codes and

devices. It refers to several sentences. The Judgment no. AP 107/2018

of ***PROVINCIA.2 of March 12, which establishes that “For their part, the clients

You have a duty of custody with respect to your access codes (...);

Judgment of the AP of Seville, dated May 26, 2014, having made

ignoring bank warnings and security notices; sit-

information from the AP of Las Palmas de Gran Canaria dated December 20,

2012, which states that if the client incurred an error caused by a third party

zero alien to the Bank and facilitated, deceived, the keys to that delinquent;

and Judgment no. 74/2010 of the Valladolid AP of March 10.

In short, and as the Agency reproduces, "(...)", data that may have been able to

do facilitate the affected party without knowing it, or those who have been allowed to

access, making it clear that access to SMS by the impersonated-

res by itself does not allow the execution of banking operations (result

pursued by supplanters).

• Probable liability of third parties unrelated to TME, such as

bank des

understood

-

The Agency recognizes that this type of scam is initiated in the field of

banking entities and their purpose is to execute banking operations.

However, it continues to attribute to TME a responsibility that it does not bear.

rresponds, but corresponds to these. TME only processes the data identified

assets of the client in order to prove the identity of the applicant of the

management and to be able to continue providing the mobile telephony service, attending

to the requirements of telecommunications and consumer regulations). But

the AEPD is trying to make it responsible for some treatment operations

personal data carried out by third parties (such as banks), which do not

are your responsibility.

The Agency acknowledges that the PSD2 Directive does not apply to TME and

insists that the duplicate SIM card allows impersonators to access

to the transaction authentication code. He insists that he is not having-

It is taken into account that the operation or treatment activity carried out, and the

which is responsible for the treatment, is limited to managing the duplication of a

SIM card within the framework of its obligations as a service provider

electronic communications. It has nothing to do with the mechanisms of autism.

tentication used by third parties.

Insists, the bank should establish security measures

suitable for access to your private environment and check that effectively

mind is sending a key to carry out the transaction to the holder of the

account and refers to the SAP of Alicante 107/2018 that indicates that "It constitutes by

both an essential obligation of the entities providing the banking service

ca online to equip itself with sufficient measures that guarantee the user the

security of operations (...) and to the SAP of Zaragoza that says: except

fraudulent act or gross negligence of the account holder, the liability

responsibility of the operation belongs to the bank to which it also corresponds

bar the proper functioning of the computer system".

In conclusion, from all of the above it can be concluded that this Agency is im-

placing TME with a series of obligations that do not correspond to it, demanding

again strict liability, for the mere fact of being the provider

of the mobile telephony service and consequently be in charge of managing

tion SIM duplicates.

• Intentional actions of third parties to commit a crime

In the Resolution Proposal, the Agency acknowledges that:

-

-

-

"(…) to complete the scam, it is necessary for a third party to "impersonate the

identity" of the owner of the data, to receive the duplicate of the card

SIM".

"SIM Swapping is a criminal technique consisting of obtaining

a duplicate of the SIM card associated with a telephone line owned by

identity of a user, in order to impersonate their identity to obtain

access to your social networks, instant messaging applications, applications

banking or electronic commerce, in order to interact and

carry out operations on your behalf, authenticating through a user

and password previously taken from that user, as well as with the

double factor authentication when receiving the confirmation SMS in your pro-

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 supplanting

fraudulently obtains the access data or the credentials

of the customer's online banking, but he needs to be able to know the

verification code, second authentication factor, to be able to

execute any operation. By the time you get the SIM card

duplicate already has access to this second factor of authentication as well

and, therefore, from that moment he can carry out the acts of disposition for

trimonial you want".

It must be taken into account that, from the commission of a crime, as indicated in the

Article 27 of the Criminal Code, those responsible are the "authors and accomplices"

ces", being authors "those who carry out the act by themselves, jointly

or through another that they use as an instrument" (article 28 CP). Y

It is clear that these authors are third parties that have nothing to do with TME.

On the other hand, we must also refer again at this point to the en-

previous win by the impersonator to the commercials of TME to

get certain things done.

It even states that it could be considered a case of force majeure, therefore,

box the circumstances described in said concept, which determines the lack responsibility or culpability in the offending conduct. alludes to 3 sentences (of the AP of Malaga and Barcelona).

In abstract given in behavior , the essential element of culpabili does not concur in this case.

- , as: of MSDs

~ Has always acted with full and well-founded belief that excludes all responsibility and in compliance with applicable legislation.

~ We are faced with the responsibility of the employees of the MSD users and providers (treatment managers) who have in-complied with the operations established by TME, despite the more than evident and proven diligence of TME within the framework of said relationship contractual.

~ In any case, and in the event of identity theft, it can produced by a multitude of factors that are beyond the will and ability action of TME, such as:

i) There are third parties who have the will to commit a crime, action which is unavoidable for Telefónica (in other words, it is not a error that can be overcome as indicated by this Agency, since there could be no

been avoided).

ii) The data that allows identity theft is not obtained

Telefónica nests. Users have an obligation to safeguard

and obtaining them may be derived from negligent action.

people of said users by giving access to said data.

iii) The banking entities are responsible for determining the

necessary security measures to guarantee the consent

of the account holder before any banking operation, and the

proof of your identity.

Therefore, it is of extraordinary interest to reiterate that in this case there is no

causal link by action or omission, between TME and the final result, due to the

intervention of third parties with sufficient entity to alter that link.

Therefore, since there is no unlawful conduct, nor typical, nor guilty of

TME in the imputed facts we insist that it should have been ordered

filed this procedure and not impose any sanction.

na.

FIFTH. BREACH OF THE PRINCIPLE OF PROPORTIONALITY

In the hypothetical case that the AEPD, lacking adequate legal support,

legal and with the sole purpose of imposing a fine, considers it appropriate and

dispensable to financially sanction TME, the amount must be

estimated taking into account in any case the principle of proportionality that

sanctioning power prevails.

It refers to the STS of June 2, 2003 and to Considerations 4, 129 and 148 and

to article 83.

The economic penalty is totally ineffective and disproportionate. In

item forecasts

Specifically, they have not taken into consideration the

83.1 and 83.2 of the RGPD when determining the amount of the administrative fine.

deal proposal.

5.1 OF THE AGGRAVANTS APPRECIATED BY THE AGENCY

- 83.2.a) GDPR.

Regarding seriousness: Adduces SAN 00496/2017, in which it is not considered fair

tified or motivated the assessment of the conduct as serious by the

SESIAD, to the extent that it was not appreciated that the breach was

widespread.

Regarding the duration: it is surprising that the Agency appreciates the aggravating circumstance of

tion, understanding that the events cover a period of more than a year, and at the same

time the lack of continued nature of the in-

fraction.

Concerning affected stakeholders: the Agency is conveniently using

the information is transferred by TME, given that, on the one hand, it rejects the arguments

elements exposed in the Third Allegation of the Allegations to the Agreement of

Home and on the other, understands that the aggravating circumstance of interested parties affected

based on the information transferred within the framework of the requirements

of information practiced.

About the damages produced: in no way can it be attributed to

TME responsibility for the materialization of bank fraud, since

your responsibility ends with the result of the duplicate card, but not

is responsible for the customer identification policies established by

banking entities.

- 83.2.b) GDPR. Negligence:

The

with the complaining parties ONE, TWO and THREE

events that occurred

can be considered in no way as a representative sample

of the level of commitment shown by TME in the fulfillment of its obligations

regulations in terms of data protection and, much less, of the degree of

effectiveness of security policies that are designed to

serve a volume of customers that exceeds 8 million.

- 83.2.d) GDPR. Responsibility:

TME does not understand the meaning of what is expressed in this aggravating circumstance nor the

used by the Agency to reach that conclusion.

- 83.2.e) GDPR. Other offenses committed:

It considers that there is only room for a restrictive interpretation of said precept,

being taken into account in any case, only those sanctions

that had previously relapsed in relation to the same type of offender.

- 83.2.g) GDPR. Data categories affected:

The AEPD is referring once again to the damage caused by fraud.

of banking, when that has nothing to do with the type of data categories

treated by MSDs that do not fall into the category of sensitive data collected

given in article 9 of the RGPD, if not that the AEPD itself classifies them as “da-

low-risk cough”, according to the category of personal data made in the

section 6.2.3 of the “Guide for the management and notification of security breaches

dad.”

- 76.2.b) LOPDGDD. Link with the realization of treatments.

Although it is true that TME carries out a high volume of treatment operations,

processing of personal data, the vast majority of these progress without further in-

incidence. It could, where appropriate, be considered the link between TME and the reality

processing of personal data as a mitigating circumstance, not as a

aggravating circumstance.

5.2 OF THE EXTENUATIVES APPRECIATED BY THIS AGENCY IN THE

START AGREEMENT

TME considers that the Agency has not taken into account the following

extenuating:

- 76.2 d) LOPDGDD. Negligence of the affected:

The impersonations of identity produced in the three cases of the parties involved

claimants would not have been possible under any circumstances if the impersonator did not

had carried out a prior illegitimate capture of the personal data of

these clients.

The Agency rejects the concurrence of this extenuating circumstance, understanding that the

cited precept "refers to a voluntary and active action of those affected,

circumstance not accredited in the analyzed cases”. However, it is not that

what the aforementioned article says, which specifically indicates that “when deciding the im-

position of an administrative fine and its amount in each individual case

will duly take into account: d) The possibility that the conduct of the affected

ted could have induced the commission of the infraction."

If the Agency understands that the fraud could have been avoided if

TME would have used different identification mechanisms (question

which has been shown to be uncertain throughout this Procedure), does not

may arbitrarily overlook the fact that fraud did not

would have taken place if the impersonators had not previously been made

with the personal data through the interested parties.

The truth is that TME cannot establish its identification policies.

covering all the scenarios in which the interested parties deal with their

own personal data.

- 83.2.j) GDPR. Certification of the company's processes in question:

TME has an accredited SGCP in accordance with the UNE standard

19601, which certifies the validity of the identity verification system of

clients in order to prevent possible crimes of fraud (art. 248, 249,

250, 251 and art. 251 bis of the Penal Code).

In the event that it cannot be taken into account to assess the attention

contained in article 83.2.j) of the RGPD, understands that it must consider

considered as a mitigating factor applicable to the circumstances of the case in

the terms set forth in article 83. 2. k) of the RGPD.

- 83.2.j) GDPR. Other mitigating factors applicable to the circumstances of the

case:

They consider that they have not been taken into account:

-. The economic losses suffered by TME: The Agency has not taken into account

that the operators are one more victim of this type of action. TME suffers so much

direct economic losses (refund of the amount of the duplicates, between

others) and indirect (serious reputational damage, high impact on the experience of

customers).

.- The complexity of implementing new measures. TME has implemented (...)

that pretend to be an important lever of change in the processes of identification

tion of clients However, this type of initiative entails great

amounts of human and financial resources, making it impossible to implement

immediate tion of the same.

.- TME has duly audited its (...) for Crime Prevention.

.- The concurrence of the obligations derived from the regulations applicable to companies

dams operating in the telecommunications sector.

For all of the above, if the AEPD decides to maintain the sanction, these mitigating factors must

be taken into account to reduce its amount.

Based on the above allegations, TME requests:

Yo.

ii.

The procedure is suspended and the claimants are required to

provide the status of the complaints filed in order to determine

nar if there is criminal prejudiciality.

The non-existence of responsibility on the part of TME for the pre-

alleged infractions imputed, ordering the filing of the sanctioned file

pain

Subsidiarily, it is taken into consideration that the

conduct in the precept that the Agency continues to consider violated, and

there is an error in the classification of the infraction.

In case of understanding that the technical and security measures are not adequate

das, the specialty of article 32 of the RGPD should be addressed.

Finally, that the initially proposed sanction be reduced.

iii.

IV.

v.

(The underlining, italics and bold are from TME).

These Allegations will be answered in the FD of this Resolution.

Of the actions carried out in this procedure and the documentation

in the file, the following have been accredited

PROVEN FACTS

FIRST: TME is responsible for the data processing referred to in the presentation.

this Resolution, since according to the definition of article 4.7 of the RGPD it is

who determines the purpose and means of the treatments carried out with the purposes

indicated in its Privacy Policy https://www.movistar.es/particulares/centro-de-

privacy/#For: At Movistar we process the data of the client or user for the provision

tion of the service, as well as for other purposes that it allows or authorizes in

the terms informed in this Privacy Policy or in the Conditions is-

specific to each contracted Movistar Product or Service.

SECOND: TME provides its mobile telephony services through three co-brands

commercials that are: Movistar, O2 and Tuenti. Each of them has different operations.

operating ratios.

THIRD: On December 13, 2019, this Agency received a claim

mation made by claimant one (file with reference number E/

00560/2020), directed against THADER, located in ***LOCATION.2 (***PROVINCE.2),

after issuing on March 6, 2019 a duplicate of the SIM card of the line

***TELEPHONE.1, in favor of a third person other than the owner of the line -the party

claimant one.

These events were reported to the Mossos d'Esquadra USC of ***LOCALI-

DAD.3 (Barcelona) on March 8, 2019, procedure number XXXXXXXX,

in which claimant one stated the following:

"(…) That he wants to report that his mobile SIM card has been duplicated again

***TELÉFONO.1 and this time, they have accessed their BBVA online banking and

made two transfers for a total value of 28,000 euros.

That the first complaint with the steps indicated above doubled the tar-

SIM card of the mobile but no fraudulent charge or movement was found.

slow through your mobile.

That he canceled his SIM card and got a new one with a new mobile number

(…)

That on the morning of 03/07/2019, the complainant received a call from

your entity to come to the office.

That once in the office they told him if he had made any strange movement

from your online banking and the complainant said no.

That from the BBVA office they told him that there had been two transfers

from your current account to a third party for a value of 13,000 and 15,000 euros.

That these transfers are made first from a checking account.

denouncer in a fixed plan to the current savings account also of the de-

announcer, and from here to a third person.

That the final checking account that receives the transfers is ES00 0000 0000

00000 0000 00000 from BBVA in the name of B.B.B.

That the transfer date is 03/06/2019 in the afternoon.

That precisely, from this day in the afternoon, the complainant stayed with the

inoperative mobile. (…)". (The Catalan translation is ours).

In relation to this claim, THADER informed this Agency that, on 6

March 2019, a SIM card change was made at the Movistar store in ***LO-

QUALITY.2, according to Movistar operations "(...)" after validating the documentation

provided: (...).

TME, informed this Agency that the issuance of the duplicate was possible due to the

concurrence of several circumstances:

1.

(...):

two.- (…).

3.- (…).

FOURTH: On December 17, 2019, this Agency received another re-

claim made by claimant one (file with reference no.

E/00560/2020), directed against MOVISTAR CARREFOUR ***PROVINCIA.1, after experience

say on February 5, 2019 a duplicate of the SIM card of the line ***TE-

LÉFONO.2, in favor of a third person other than the owner of the line -the re-

crying one-

These events were the subject of a complaint before the Mossos d'Esquadra USC of

***LOCATION.3 (Barcelona) on February 7, 2019, with procedure number

cia XXXXXXXXXX, in which claimant one stated the following:

“That on the morning of 02/05/2019 he received a call from a Mo-

visit from ***PROVINCIA.2 with telephone number XXXXXXX in which he was informed that

a person was requesting a SIM card duplicate of the phone number

phone ***TELEPHONE.2, which corresponds to the declarant.

That specifically they told him that an Italian person had gone to five

Movistar stores in ***PROVINCIA.2 requesting a duplicate SIM card

of the number ***TELÉFONO.2 and brought a complaint in which he said that he had

lost your mobile phone with phone number XXXXXXXXX.

That they also told him that at the time they asked for his DNI this

boy was leaving the store.

That those from the same Movistar store asked him if he had authorized a

duplicate card.

That the declarant answered no.

That on today's date the declarant has gone to the Movistar store in ***LOCALI-

DAD.3 and they have informed him that yesterday at 9:48 p.m. in a Carrefour in

***PROVINCIA.1 had made a duplicate of the card with their phone number.

phone.

That the distributor code where it was made is ***CODE.1 and the number of

agent who made the duplicate is ***AGENT.1.

That they also informed him that at the time the duplicate was made he

He was left without a telephone line since they discharged him." (The Catalan translation is

our).

In relation to this claim, TME informed this Agency that the duplicate never

ca came to be carried out in full, since the distributor did not deliver the card

SIM to the impersonator. (...).

FIFTH: On March 6, 2020, a claim was received by this Agency

tion made by the complaining party two (file with reference number E/

03543/2020), directed against CATPHONE and TME, after being issued on February 13

of 2020, a duplicate of the SIM card of the ***TELÉFONO.3 line, in favor of a

third person other than the owner of the line -the claimant party two-.

These events were the subject of two complaints before Post P. de las Rozas of the Co-

mandate of the Civil Guard of Madrid on February 13 and 18, 2020, with

attestation numbers ***ATESTADO.1 and ***ATESTADO.2 respectively, in which

Claimant two stated the following:

In the first complaint:

"(…) a duplicate of the SIM card of the telephone ***TELÉFONO.3 no

authorized by the complainant, that the complainant about 1:00 p.m. when making a

call from your phone this does not allow you to make it.

That he begins to take steps, he gets in touch with TELEFONICA MOVIS-

TAR which inform you that you have made a duplicate card IN A STORE-

DA DE MOVISTAR located at ***ADDRESS.2 of the town of ***LOCATION.4.

That the complainant informs him that he is in Madrid and it is impossible for him to

have authorized any duplicates.

That having well-founded suspicions that this was not normal, he performs checks

deposits in your bank account of BANCO SANTANDER which is at your

name, observing several unauthorized charges in it, these being the following:

following:

They have made a purchase in the REVOLUT company worth 2,500 euros

They have made a purchase from the REVOLUT company worth 3,500 euros.

(...) that he received a message on Monday, February 3 from his bank from (...) his account manager

Santander bank asking him to contact the telephone number ***TELÉ-

FONO.4 and that on the 10th he received a call from the Bank's anti-fraud department

Santander informing him that there was an attempt to manipulate accounts from

***COUNTRY.1, who went to the bank and changed the passwords."

In the second complaint:

"(...) you want to expand the data of the charges suffered on your card since they have made you

filed more charges of which he was not informed the day he made the complaint.

That on February 13, 2020, when he was reviewing his accounts, he observed that they had

made some charges which you have not made or authorized in your bank account

***ACCOUNT.1 and associated card number ***ACCOUNT.2, for a value of:

REVOLUT company, 02-13-2020, worth 2,500 euros

REVOLUT Company, 02-13-2020, for a value of 5,500 euros

That same day they have carried out the same procedure in another account that has

with the bank ES00 0000 0000 0000 0000 0000 and card number

associated card ***CARD.1 , for a value of:

REVOLUT Company, 02-13-2020, for a value of 2,450 euros

REVOLUT Company, 02-13-2020, for a value of 3,500 euros"

In relation to this claim, TME verified to this Agency that there was a request

tude of (...) on February 13, 2020 at 11:48 a.m. through (...) ***LOCALI-

DAD.4" and that that same day at 5:12 p.m., a request was made for (…) "(…)".

SIXTH: On October 23, 2020, a claim was received by this Agency

tion made by claimant three (file with reference number E/

09638/2020), directed against TME, after being issued on September 25, 2020,

a duplicate of the SIM card of the line ***TELÉFONO.5, in favor of a third party

sona different from the owner of the line -the claimant party three-.

On September 25, 2020, at 2:40 p.m., the complaining party received three

He received an email sent by movistarcloud@telefonica.com with the Subject:

Confirmation of cancellation in Movistar Cloud.

On that same date, at 2:53 p.m., claimant three responded manifestly

stating that: "I have not canceled the subscription. It was an error or an unauthorized use

do of someone Please contact me. ***PHONE.5"

On September 26, 2020, the three complaining party consulted the application

TME website and found that the owner of the line ***TELÉFONO.5 was Mr. F.-

F.F. with NIE: ***NIE.1.

There is evidence of the recording of the change of ownership of the service requested on the 25th of

September 2020 -with a duration of 02:12 seconds-, by Mr. F.F.F. with NIE:

***NIE.1, in which you provide your personal data (name, surnames and NIE) and the data

personal information of the claimant three (name, surnames, DNI, landline telephone number

and telephone number of the two mobile lines).

Due to these facts, claimant three filed three complaints with Post P.

de las Rozas of the Madrid Civil Guard Command on the 28th and 30th of

September 2020 and October 2, 2020, with certificate numbers XXXXXXXXX,

XXXXXXXXXX and XXXXXXXXXX respectively, in which he stated the following:

In the first complaint:

“A total of three charges have been made on the due card, subtracting

a total of 1200 euros.

A total of six charges have been made to the debit card, subtracting a total

of 3899 euros.

They have also made a transfer to him through BIZUM of 500 euros, destined for

swam to a certain E.E.E. with telephone number ***TELÉFONO.6 and a bank recharge-

ria of 1400 euros.

All this makes a total of 6699 euros.

The complainant states the possible modus operandi of the author: That through a

of a change of name of the holder in his contract, for the line belonging to the number

number ***TELEPHONE.5, with MOVISTAR by telephone, without your consent, the

The possible author made the change, requesting a SIM card from said company. nullifying

the complainant's SIM card.

That after obtaining said SIM card, the author made the bank transactions through

through a mobile phone, because after carrying out any operation with the entity

banking entity, you need the approval via SMS of the telephone number that makes the

operation.

After this, the possible author got into the application of the Santan-

der and through I HAVE FORGOTTEN MY PASSWORD, said bank sends SMS to

phone number associated with the bank account.

That the change of holder of the MOVISTAR account, the complainant provides data

of the possible author: F.F.F.***NIE.1.

It also provides a bank transfer of 4,998 euros that was cancelled, which was

addressed to a certain XXXXXXXXXXX, being the account number ES00 0000 0000

0000 0000 0000 of the banking entity CAIXABANK SA.

That the complainant provides the fraudulent MOVISTAR contract with the name and

surnames of the alleged perpetrator, copy of the last invoice of the legal contract of the denouncer,

customer, details of the aborted transfer and the charges made."

In the second complaint:

"Be a person in these dependencies D. D.D.D. to make the following correction

about the complaint filed.

That in the proceeding entitled PROCEEDINGS TO START FOR A COMPLAINT OF INFRINGEMENT

CRIMINAL MENTION THROUGH APPEARANCE in its eleventh paragraph where it is expressed

sa that all this makes a total of 6699 euros should put that all this makes a

total of 6999 euros."

In the third complaint:

“(…) That on Thursday 10-01-2020 the complainant appeared at his office in the

Banco Sabadell located in (...) to recover the passwords previously blocked for

be able to operate.

That Banco Sabadell reported that unfortunately a transfer had been issued

fraudulent payment amounting to 7,003.00 euros in the name of H.H.H. to the account

ES00 0000 0000 0000 0000 0000 of the banking entity ING reason for which

is forced to report the facts in order to recover the amount defrauded.”

In relation to this claim, TME informed this Agency that, on September 25,

In the month of 2020, there was (...), but it only made the change effective in the line ***TELÉ-

PHONE.5.

SEVENTH: The four complaints filed affect customers of the Mo- brand

view

EIGHTH: TME accounts for the Movistar brand with (...).

TME requires (...).

NINTH: TME counts for the Movistar brand with a (...).

TENTH: TME signs, (...)

.

ELEVEN: In the content of the "(...)", signed with (...), it is provided:

(...).

TWELFTH: TME signs,(…).

In the first clause it provides (...).

In the second clause it provides (...):

(...).

THIRTEENTH: On date (...) TME adds a (...)", which are written in

the following terms:

(…)

FOURTEENTH: The content of (...) provides:

(…)

RESPONSIBILITY.

1. (…).

(...).

FIFTEENTH: TME signs with (...)

.

SIXTEENTH: TME sent a (...).

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.

The allegation referred to the initiation of the sanctioning procedure is dismissed.

because the AEPD has acted in accordance with the general principles of article 3.1

of the LRJSP, among which is the effective service to citizens, good faith,

legitimate expectations or the transparency of administrative action.

Of the participation of the telecommunications operators, and the other interveners

and of the conclusions or agreements reached in the WG and that appear in the

corresponding minutes, it cannot be deduced that the AEPD has validated

do any type of action of TME in relation to the facts object of analysis in the

present procedure.

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 are exercised by the administrative bodies that have them attributed.

you give as your 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 that has directly affected the duty to maintain confidentiality.

confidentiality of customer data.

Thus, and taking into account the above considerations, no appearance

of legality in the performance of TME can be inferred from the participation in the aforementioned

GT. So much so that, in the allegations, he limited himself to highlighting his participation, but not

did not specify or determine to what extent the AEPD communicated one thing and then did another,

in the sense of what specific aspect he drew from participation in the aforementioned group,

which has subsequently been contradicted by the initiation of this disciplinary proceeding.

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 had the purpose of analyzing the

procedures followed to manage SIM change requests by

TME, identifying the vulnerabilities that could exist in the operating 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 facts declared previously proven, violate article 5.1.f) of the RGPD and

are constitutive of the infringement provided for in article 83.5.a) of the RGPD that we consider

ra very serious infraction the violation of:

"the basic principles for treatment, including the conditions for the

consent under articles 5, 6, 7 and 9,"

Likewise, it is classified as sanctioned 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:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

61/106

“The processing of personal data violating the principles and guarantees established

established in 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 TME had documented policies

data protection regulations in which the way of acting of TME and of

those in charge, before the processing of personal data necessary for the provision

tion of the contracted services and throughout their life cycle. However, also

It was proven that adequate safety in the treatment had not been guaranteed.

processing of personal data, taking into account the result produced by the impersonation

tion of identity

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 analysis, planning, establishment

maintenance, updating and control of data protection policies in

an organization, especially if it is a large company, -understood as the set-

set of guidelines that govern the performance of an organization, practices, procedures

and tools, among others-, from privacy by design and by default, which

guarantee compliance with the RGPD, that prevent the materialization of risks and

that allow the controller to demonstrate compliance.

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 TME, it was verified, among others, the implementation of a model
most effective phishing risk avoidance, review, enforcement, and
improvement of the security measures applied in the different channels aimed at
ensure the procedure of identification and delivery of the SIM card, in order to
prevent the materialization of fraud. Also, the immediate reaction to the
described facts and the ability of the operator to demonstrate compliance. By
all of the above, we focus the facts on the infraction derived from article 5.1.f) of the
GDPR.

Notwithstanding the foregoing, in accordance with the principle of proactive responsibility itself, it is the
The person responsible for the treatment must determine what the security measures are.

to be implemented, since only the latter has in-depth knowledge of its organization.

tion, the treatments it carries out, the risks associated with them and the

the precise security measures to be implemented to make effective the principle of in-

integrity and confidentiality.

However, it has been proven that the measures implemented by TME were insufficient.

and not only because they have been overcome and the transfer of personal data

nals to a third party.

In a non-exhaustive way and by way of example, we will look at (...), a previous step

in many cases to obtain a duplicate SIM card.

Thus, from the documentation sent by TME it is inferred that the personal data associated

two to the security policy are (...) be formulated with respect to some data that co-

know only the operator and his client. No supplementary requirement was required.

Dear.

We have to mean that, in the case of claimant three, it was enough that the sub-

planter will provide the (...), of the claimant party three to seek the change of

ownership. (...).

Likewise, (…).

On the other hand, and in terms of the means used to identify the owner in person,

owner of the line in order to obtain a duplicate SIM card, (...).

Especially significant is the case of the complaining party one in which (...) for

get the duplicate SIM card. Thus, from the presumed representative and impersonator

is accepted (...).

As for the change in the offending type that the AEPD had been habitually imputing in

the cases in which the fraudsters managed to supplant the identity of the clients

for different purposes (article 6.1 RGPD), and the imputation to TME of the responsibility
reliability of the result of the fraud carried out by a third party, we must indicate that the
AEPD has attributed, by virtue of articles 57 and 58 of the RGPD, information functions
investigation, as appropriate, regarding the claims presented to the
effect.

In the case now examined, the AEPD, after carrying out the investigations
timely and in relation to a series of specific facts that it considers proven,
incardinates them in the offending type that it considers appropriate, according to the application
tion and interpretation of the regulations, motivating such action in a detailed and sufficient manner.
tuation. And it is that the AEPD, like the rest of the public powers, is linked to the
principle of legality (article 9.1 and 9.3 Constitution -CE-) that implies the application and
interpretation of the norms according to the assumption of specific fact that concurs
in each case.

TME cites in its defense a series of resolutions issued by the AEPD. As well,
in PS/00114/2019, he was sanctioned for contracting without accrediting the representation
sitting. Regarding PS/00453/2019, it was sanctioned for the fraudulent hiring of
new telephone lines, without in that case producing a duplicate of a
SIM card with respect to a pre-existing telephone line belonging to another holder
(since it was the contracting of a new line that lacked a headline
previous). Finally, PS/00235/2020 was sanctioned for lack of diligence in the application
cation of the principle of legality.

It should be noted that TME does not explain to what extent your rights are affected
of defense and procedural for subsuming the facts in article 5.1 f) and not in the

article 6.1 of the RGPD.

Alleges a proscribed legal uncertainty or the violation of the right of defense, without

However, the AEPD has guaranteed the rights provided for in article 64.2.f) and 89.2

of the LPACAP, among which is the right to make allegations, without,

therefore, it can plead helplessness. He has been able to allege and contribute to the procedure

what you have agreed to by law, without any limitation on the part of the AEPD. All

the allegations made to this effect have been considered and answered.

Furthermore, let us remember that treating personal data without a legal basis,

that is to say, without the legitimizing assumptions foreseen in the aforementioned precept, it has as

consequently an unlawful treatment, that is, contrary to paragraph 1 of article 5 of the

GDPR. At that time, the same precept that is imputed in the case analyzed and, in any

In any case, in the face of a hypothetical imputation of article 6.1, as TME maintains, also

Article 85.3 a) of the RGPD would also apply. Ultimately, TME does not determine

as their procedural situation may be aggravated by said legal qualification, instead

gar of which it maintains, beyond affirming that the Agency incurs in arbitrariness.

On the other hand, it is perfectly admissible that the AEPD has considered the violation

tion of a certain precept in the conviction that it is more in line with the

events that occur, without this action being able to be described as arbitrary, especially

when properly motivated. At the beginning of this FD we already indicated that the actions

The Agency's hearings were intended to analyze the procedures applied to the

SIM card change requests. The SIM card constitutes the physical support through

through which the personal data of the affected person is accessed. But

its provision and control, access to the owner's personal data, as well as

such as the possible use or uses by third parties, becomes a threat that can

have devastating effects on the lives of these people.

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,
rias 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 certain requirements
sites that, although a quick reading may seem very strict, a reading
much more carefully it has been shown that they were not. With which, the scam or su-
plantation, which apparently could seem complex and difficult, it is observed that it is not
It has been both due to the inadequacy of the security measures at the time of surveillance
that it is the owner of the SIM card or the person authorized by him who requests the
duplicate.

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 identified natural person.

testable (“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

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

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

physical, 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

undermines the purposes and means of the treatment, the person in charge of the treatment or the criteria

specific for their appointment may be established by the Law of the Union or of the

Member states".

8) “in charge of the treatment” or “in charge”: the natural or legal person, authority

public, service or other body that processes personal data on behalf of the person in charge.

ble of the treatment;

TELEFÓNICA MÓVILES ESPAÑA, S.A.U., is responsible for the processing of

data referred to in the exposed antecedents, since according to the definition

of article 4.7 of the RGPD is the one that determines the purpose and means of the treatments

made with the purposes indicated in its Privacy Policy: In Movistar tra-

We store the data of the client or user for the provision of the service, as well as for

other purposes that the same allows or authorizes in the terms informed in the

this Privacy Policy or in the specific Conditions of each Product or

Contracted Movistar service.

(...); CATHPONE-NET, S.L and THADER TELECOMUNICACIONES S.L, act in the

status of treatment managers.

In addition, the issuance of a duplicate SIM card implies the processing of 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 by

you 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 Services Digital Network - Mobile Station Network

Integrated Services Digital-), 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 (hereinafter, Law 25/2007),
requires that holders of all SIM cards, whether prepaid or contract, be
be duly identified and registered. This is important because the identification
cation of the subscriber will be essential to register the SIM card, which entails
It will be necessary that when obtaining a duplicate of this, the person requesting it must
also identify themselves and that their 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 TME:
PREVIOUS: ON THE INITIATION OF THE PUNISHING PROCEEDINGS.
In Antecedent Four we made reference to the four requirements of
information addressed to TME on different dates that were the object of the co-
corresponding notification, consequently, it cannot allege its ignorance
I lie.
The SAN of the Contentious-administrative Chamber, sec 1ª, 10-17-07 (rec
180/06) justifies the convenience of the preliminary investigation actions

in relation to sanctioning procedures stating that: “It is about

that due to the seriousness and transcendence that the exercise of the power

sanctioning, since the legal status of someone who is subjected to an experiment

sanctioning tooth, for this single circumstance, can be negatively

mind affected, it is necessary that the decision to initiate the procedure

sanctioning party is founded and based on solid reasons that require such

initiation”.

That is, in order to allow the sanctioning body to know the facts

predictably offending parties, the concurrent circumstances and the people

intervening, it is allowed to carry out said actions or inquiries

prior assessments, insofar as they are necessary and timely to verify, to what extent

point, there is a rational basis to understand that the infringing act occurred, and im-

put it on a certain person.

Regarding the violation of the principle of good faith and legitimate expectations,

your appreciation is up for it.

The principle of legitimate expectations, contained in article 3.1.e) of the LRJSP,

principle that, as the jurisprudence -SSTS of December 28 has reiterated

2012 (Rec. 273/2009), July 3, 2013 (Rec. 2511/2011), among many others-

"cannot be invoked to create, maintain or extend, within the scope of the Law

public cho, situations contrary to the legal system", being the plaintiff

responsible for the infractions appreciated in the Resolution Proposal, to

tenor of article 28.1 of the LRJSP.

In relation to this principle, the SAN, of April 29, 2019, RJCA 2019\449, indicates

ca: According to what was declared by the aforementioned judgment of July 6

2012 (RJ 2012, 7760) the principle of legitimate expectations implies that "the

public authority cannot adopt measures that are contrary to the

hope induced by the reasonable stability in the decisions of the former, and

on the basis of which individuals have adopted certain decisions

nes. (...) as stated in the judgment of July 3, 2012 (RJ 2012,

11345) (appeal 6558/2010): "(...) The protection of legitimate expectations does not

encompasses any kind of subjective psychological conviction in particular, meaning

do only that <confidence> on aspects that can be protected

concrete, based on signs or external facts produced by the Administration

nistration sufficiently conclusive..." But from the decisions of the

this Chamber, it must be concluded in an important and relevant element to confirm

ensure legitimate expectations, namely, that the specific action expected

in that trust is in accordance with the Law (judgment last cited-

da), that is, it is necessary that the performance of the Administration, with its con-

conduct, induce the administrator "to believe that the action he develops is

lawful and adequate in Law" (judgment of July 3, 2012, issued in the

appeal 6558/2010). In the same sense, it has been declared that it cannot

rely on legitimate expectations "the mere expectation of an invariability

of the circumstances", as stated in the judgment of March 22,

2012 (appeal 2998/2008), in which it is concluded that it cannot be maintained

irreversible behavior that is considered unfair.

In short, the participation of TME in the GT does not modify the responsibility

which is now charged. Therefore, due to the fact that he participated in

a GT whose objective is to tackle such a specific criminal activity (“SIM

Swapping”), does not prevent that once an infraction is verified, it must

be sanctioned

Indeed, the competencies, functions and powers attributed to the

AEPD, are exercised in accordance with the legal system following the "Principles

General” of article 3 of the LRJSP, among which are the objectivity

integrity and transparency of administrative action, which apply to the AEPD, in

its status as a public law entity, specifically, an administrative authority

statewide independent investigation, article 109 LRJSP and 44.1 of the

LOPDGDD, with legal personality and full public and private capacity,

that acts with full independence from the public powers in the exercise of

its functions.

The condition of MSD victim is not discussed, but the unauthorized access to

a duplicate SIM card, which is considered particularly serious since

enables identity theft with a purpose, to interact and

perform transactions on behalf of a third party.

I. ABOUT THE FACTS GIVING RISE TO THE INITIATION.

Question of criminal prejudiciality.-

There is no place for the deducted request because the information was already required during

during the investigation of the procedure and it was found that there was no identity

of subject, fact and foundation (article 31.1 LRJSP), budget without which

criminal prejudiciality does not concur.

Article 31.1 of the LRJSP establishes that "the perpetrators may not be sanctioned

those that have been penalized or administratively, in the cases in which

appreciate identity of the subject, fact and foundation".

In the same sense, article 77.4 of the LPACAP provides: "In the procedures

penalties, the declared facts proven by resolution

Firm criminal judicial decisions will bind the Public Administrations

regarding the sanctioning procedures that they substantiate".

Thus, the SAN of September 25, 2019, of the Contentious-Administrative Chamber

nistrative, Section 1 (Rec. 1122/2018) determines that: “The triple identity of

subject, fact and foundation between the administrative infraction and the infraction

that could correspond constitutes an inescapable requirement so that

the defendant Administration is obliged to suspend the procedure

sanctioning administrative proceeding”.

In this same judgment, in which the request for suspension of

sion of the appeal for criminal prejudiciality, an identical assumption arises

now examined, where "The recurring society is founded on the existence of

criminal prejudiciality in the existence of two complaints filed with the

National Police. Well, with the above, in the first place, it is not credited

If the processing of said complaints continues or they have been archived, or if

want, if preliminary proceedings have been initiated by any jurisdictional body,

and, on the other hand, there is no identity of the subject, since the offending subject is obvious

that it would not be the same. Thus, in relation to infractions of the LOPD (LA

LAW 4633/1999) the controller is the AVON entity, while the controller

criminal saber of a possible crime of usurpation of marital status or fraud would be

the third party who would have passed himself off as the complainant, so that with the di-

cho is sufficient to dismiss the ground of challenge that we are

analyzing. The same can be said with respect to the preliminary investigations

mitan in the Court of Instruction no. 11 in Madrid, for an attack on the sys-

AVON computer issues.

The AEPD has not ignored the content of the investigations that are being carried out

carried out, but it has been reported about people criminally

responsible for the reported crimes and has verified that he did not

There are legal assumptions to apply the precept invoked. The Senten-

claims (no. 2249/2016 and no. 1907/2017), refer to procedures

judicial in different orders, criminal and contentious-administrative. In this

case, the circumstances are different, we are in the administrative process and before the

criminal court order. In fact, TME literally acknowledges that “there is no

identity of subjects.

In short, with respect to the facts denounced and those that have been the object of the

disciplinary proceedings, it is clearly noted that there is no concurrence between some

and others the triple identity expressed, because in this sanctioning file it

that is elucidated is, if TME has carried out the treatment of the data of

personal character respecting the principles related to the treatment (article

5.1.f) RGPD), an issue outside the purpose of the criminal proceedings that are substantiated

hundred, which, on the other hand, protect different legal assets (for example:

article 248.2 of the Penal Code in relation to article 249 of the same text

legal).

FIRST. OF THE CONDITION OF TME AS RESPONSIBLE FOR THE TRA-

PROCESSING AND DELIMITATION OF PROCESSING OPERATIONS.

The Agency is surprised by the fact that it claims that we have not delimited the

operations or treatment activities when the Legal Basis

(FD) Fourth of the Motion for a Resolution is headed “Treatment of

personal data and data controller” that says: “(…) the issuance of

a duplicate SIM card supposes the treatment of the personal data of

its owner” and identifies the person responsible for this “TELEFÓNICA MÓVILES ESPA-

ÑA, S.A.U, is responsible for the data processing referred to in the foregoing.

exposed background”.

In the Third FD of this Resolution, the object of the actions was outlined:

analyze the procedures followed to manage change requests

of SIM by TME, not by other entities, such as financial ones, which

voca.

The SIM card identifies a phone number and this number, in turn, identifies

fica to its owner. 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" used in article 3, paragraph 1, of the Directive

tiva 95/46 includes, according to the definition in article 2,

letter a), of said Directive "all information about an identifiable natural person

identifiable." This concept includes, without a doubt, the name of a person.

ring next to your phone number or other information regarding your conditions.

tions of work or his hobbies”.

Also, this opinion is singled out in relation to telephone devices.

mobile phone that allow the location of the interested party, in Opinion 13/2011

about geolocation services on smart mobile devices

(WP185 document):

“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 procedure

specific for the change of SIM called for the Movistar brand “Cam-

SIM card bio”.

It refers to the CEPD Guidelines 07/2020, and the CJEU Judgment of

July 29, 2019 to highlight that the status of controller of the traffic-

processing may be limited to a particular stage of processing and that

cannot be held responsible for illegitimate accesses occurring at sea.

of the provision of services of any company that verifies the identity

your customers via mobile phone. Well, we insist, that

The only thing that has been questioned in this procedure is the adequacy of the

security measures implemented by TME for the correct identification

of customers at the time of issuing the duplicate SIM card.

SECOND. ON THE ADOPTION OF TECHNICAL AND ORGANIZATIONAL MEASURES

YOU GO APPROPRIATE.

2.1

TECHNICAL AND ORGANIZATIONAL MEASURES IMPLEMENTED

It was proven in the instruction of the procedure that there was no guarantee

ensured adequate security in the processing of personal data,

due account of the result produced by identity theft. Namely,

a third party managed to gain access to the personal data of the holders of the

lines without the security measures that TME claimed existed, hu-

They could have prevented it.

Therefore, and in view of the result produced, we were not facing a

demonstration by TME of compliance with the principles relating to the

processing of affected personal data.

Regarding the fact that the Agency does not clarify at any time why it considers the

contrary to the Regulation, the RGPD is based on the principle of res-

active responsibility and in relation to the previous regulation of the Organic Law

15/1999, of December 13, on the Protection of Personal Data and

Royal Decree 1720/2007, of December 21, which approves the Re-

regulation of development of the Organic Law 15/1999, of December 13, of

protection of personal data, where it existed in regard to

security a list or checklist system, now he is responsible for the treatment

and in charge, where appropriate, who must adapt the implementation of

security measures to the specific type of treatment carried out, and precisely

therefore, not because of the non-existence of security measures - a circumstance that

concurs in this case - but because of those that TME had, they were not

adequate to avoid the events that occurred.

Similarly, as a result of the investigation of the procedure, it has been verified

actively and continuously applying new measures to promote

view and ensure data protection in the issuance of duplicates

or even in other treatments such as the "Change of owner" operation, whose

The last update has occurred on August 28, 2021.

TME has been found to improve the effectiveness of all procedures.

commanding actions, corrections, introducing changes and reinforcements to improve

continually reduce the provision of this service or others related to it.

It has implemented an accountability policy and has made an effort to demonstrate

bring its fulfillment. It has documented the decisions adopted in relation to

tion with the treatment, audits and reviews the security of the information and has

provided the Agency with information regarding the safety of the treatment.

From all this, from the attached documentation and as we analyze in the FD

Third, although compliance with the principle of responsibility is concluded

proactive, notwithstanding all of the above, administrative responsibility is

required according to the Proven Facts and FD of this Resolution.

Recital 78 RGPD declares "... the data controller must

adopt internal policies…" and article 24.2 establishes "When they are pro-

portioned … the application … data protection policies", and that go

beyond the reference to the formal aspect of the existence of a document

entitled "Data Protection Policy" where the mere reproduction is made

formal tion of the articles of the RGPD and is reduced to a mere declaration of the

Willingness of the person in charge to commit to regulatory compliance.

Therefore, the current internal security policy applied by TME is

consistent with the PSD2 Directive that requires the adoption of "authentication" systems.

enhanced client information, despite not being included in its scope of application

(article 2).

The same statement must be made regarding the "Ex officio inspection plan

on distance contracting in telecommunications and commercial operators

energy cializers" that contains recommendations on "Verification

identification of the client's identity in subsequent processes" and that TME applies to

its procedures:

In the Customer Area of the website, customers identify themselves and authenticate

through user code and password. Because a client can

have contracted more than one line, the user code can be numbered

line number (access only to the data associated with the queried line) or DNI

(access to all the data associated with the lines contracted by the user)

river) In the Customer Service departments (telephone channel) of the

different companies, the client is usually identified by full name,

DNI and a third random data such as the address to which the invoices are sent

or bank account number, although many companies provide

a password (at the request of the client) that must be indicated to pro-

give access to the data.

Regarding the following statements:

1.- TME (...), it is only possible to request it in person at the store.

Let us remember that in the case of the complaining party three there was

(...) and made the change effective on the line ***TELEPHONE.5.

3.- (…). We refer to the proven facts that have affected

the complaining party three.

2.2 REVIEW AND UPDATING OF TECHNICAL AND ORGANIZATIONAL MEASURES

IMPLEMENTED NIZATIVES

Undoubtedly, in the investigation of the file it has been revealed

review of technical and organizational measures.

TME has reinforced the operations applicable to the different channels and has introduced

improvements have been made in order to prevent the recurrence of similar events. Dis-

puts (...).

It also recognizes the implementation of (...) systems.

All these measures and constant adaptation efforts based on the

new risks will be considered in the condition of “mitigation”.

you”.

2.3 ASSESSMENT OF THE ADEQUACY, TIMELINESS AND EFFECTIVENESS OF

THE TECHNICAL AND ORGANIZATIONAL MEASURES IMPLEMENTED

The cases declared by TME during the 2019 and 2020 financial years are a re-

reflection of the adequacy, timeliness and effectiveness of the measures adopted and im-

supplemented after the start of the actions carried out by the

Agency.

TME recognizes that fraud has decreased by 71% in that period. Remember-

We state that the first requirement of the AEPD is dated January 13,

2020.

If we look at the data provided by TME, the figures by themselves express

determine the effectiveness of recently adopted security measures,

due precisely to the introduction of others other than the pre-existing ones, which

have been more appropriate, timely and effective.

(...).

He reproaches the Agency for not stopping to assess these aspects.

Precisely, the imputation that is finally made against TME in Pro-

Resolution is referred -only- to article 5.1.f) and not to 5.2

GDPR, as initially considered in the initiation agreement. This alter-

ration has had a direct effect on the sanction that was initially considered

and that amounted to 2,000,000'00. And this is so, due to the assessment made (we

we refer to the Third FD and to section 2.1 of the allegations) by the Agency.

The security measures must guarantee that in our organization, or

in those of those with which it is subcontracted, personal data

are only used for the legitimate purpose for which they were collected, except for possible ex-

legal exceptions. Periodic checks must be carried out to verify

and assess the effectiveness of the security measures that we have implemented

do.

And of course there is an application cost, which requires time,

which in turn must be in accordance with the regulations and the state of the art,

but it is that, to select the appropriate security measures, the res-

responsible must be based on the risks to natural persons, as well as on

what is reasonable and technically possible. Article 28.2.a) of LOPDGDD

establishes some assumptions in which it already warns that it is necessary to contemplate

take greater risks than those that the person in charge could estimate if he only had
take into account their own interests (identity usurpation, economic damages,
monkeys…).
It must be remembered that the right to data protection derives from the EC,
that establishes the limitation of the use of informatics by the Law to guarantee
honor and personal and family privacy of citizens and the full exercise
exercise of their rights (article 18.4).
The Constitutional Court stated in its Judgment 94/1998, of May 4, that
We are faced with a fundamental right to data protection by the
that the person is guaranteed control over their data, any data
personal, and on their use and destination, to avoid illicit traffic of the same
mos or harmful to the dignity and rights of those affected; thus,
The right to data protection is configured as a faculty of the citizen

harm to object to certain personal data being used to
purposes other than the one that justified its obtaining.
For its part, in Judgment 292/2000, of November 30, it considers it
as an autonomous and independent right that consists of a power of dis-
position and control over personal data that empowers the person to
decide which of these data to provide to a third party, be it the State or a
particular, or which can this third party collect, and that also allows the individual
viduo to know who owns these personal data and for what, being able to oppose-

be to that possession or use.

Regarding the certification it holds for having implemented a SGCP based on

endorsed in the UNE 19601 Standard, and given that it contains surveillance and con-

control suitable to prevent crimes and to significantly reduce the risk

to commit them, the AEPD takes it into account in the condition of "mitigating".

Finally, the AEPD has not said that TME applies a policy called

Know Your Costumer, but these policies are known as such. The ther-

mino refers to the processes of identification or identity verification

that companies, especially financial institutions, but also

of telecommunications, establish to guarantee the identity of the client.

THIRD. OF THE RESPONSIBILITY OF TME IN CASES OF SU-

PLANTATION OF IDENTITY OF THE THREE CLAIMANTS

3.1 RESPONSIBILITY OF THE DATA PROCESSOR

Regardless of the considerations that TME makes about its due diligence

in the selection and delivery of instructions to the supplier, the legal precepts mentioned

tioned to dismiss their responsibility are the following:

- First of all, article 28 RGPD. In section 3.c) and 10. That is, according to

TME, the RGPD itself provides that when the person in charge of the treatment treats the

personal data in breach of the instructions of the person in charge, becomes

in responsible.

In relation to this argument, it should be noted that in this file there was never

the possibility of a company resorting to outsourcing techniques has been discussed.

lization (“outsourcing”) for the management of certain processes. I do not know

objects to the consideration of "in charge of the treatment" of the companies of

which TME uses for said management.

Indeed, it has been proven throughout the investigation that TME has found

recommended the management by certain companies of the following activities
lives:
o THADER TELECOMUNICACIONES S.L and CATHPONE-NET, S.L, ac-
would act as distributors in physical establishments, to capture
tion of clients and execution by these of certain procedures in
their contractual relationship with the operator (among them, the issuance of du-

SIM card applications).
or (...), as a management company of a call attention center (“call
center”) through which the telephone attention to customers would be carried out.
operator tees. As far as this file is concerned, through said
attention, steps of contractual relevance could be carried out, such as the
change of ownership of a telephone line.
In relation to these aspects, and the invocation by TME of the article
28 RGPD, it is necessary to indicate initially that the obligations must be defined
established in article 28.3.d) (adopt the necessary measures by the
in charge of the treatment) of the provision established in section 10 of the
same item.
Indeed, the latter establishes the following:
"Notwithstanding the provisions of articles 82, 83 and 84, if a manager
of the treatment infringes this Regulation when determining the purposes and
means of treatment, will be considered responsible for the treatment with

regarding said treatment.

From the beginning it must be ruled out that this precept allows the attribution of

sanctioning responsibility of the person in charge. Firstly, because it clarifies that

the provisions of the same is “without prejudice to the provisions of articles 82,

83 and 84” (RGPD sanctioning regime). And, above all, because the consequence

legal provision in article 28.10 is not the sanctioning one, but the one of

rar the person in charge as responsible for the treatment. The conclusion is logical

since if he violates the Regulations "when determining the means and ends

of the treatment”, must be considered as responsible.

That is not what has happened in this file. In fact, there is no

accredited that none of the three companies has carried out actions that

involved a "determination of ends and means", but, in the words of

the TME itself, would have failed to comply with any of the instructions issued by

It is in the customer identification processes.

Consequently, in no case can article 28.10 RGPD be invoked to

a presumed attribution of responsibility to those in charge, who also im-

apply the exoneration of the person responsible for the treatment (TME according to what has been

given proven in this file).

-

Invokes CEPD Guidelines 07/2020. Specifically, section 9:

This section is limited to determining, in a generic way, that both the responsible

as the person in charge of the treatment can be sanctioned for the non-compliance

compliance with the provisions of the RGPD. Nothing adds to what is already established in the

internal regulations (LOPDGDD), in which article 70.1.a) and b) includes the res-

responsible and in charge of the treatments among the sanctionable subjects.

The mere existence of both figures does not displace the manager all the responsibility.

reliability in the processing of personal data. Proceed now, therefore-

elucidate if in this case, if the obligations of the person responsible have been violated.

ble or manager.

In this regard, it was already indicated in the Motion for a Resolution that in the three

so, those in charge act on behalf of TME, in the case of (...).

That is to say, the instrumental intervention of those in charge has as its purpose the

initiation or modification of contractual relations between TME and users

end users of electronic communications services. In this regard,

It is convenient to go to the sectoral legislation, whose LGTEL establishes the following:

o Electronic communications services are considered

of "services of general interest". Let us not forget that through these ser-

vices, connectivity to services as important as the

landline, mobile or Internet access. (article 2.1 LGTEL)

o The marketing and distribution channels referred to in this ex-

pending (points of sale and call center) are established

established for the exercise by the end users of the relationships

contractual obligations with the operator. Therefore, they refer to the exercise

of the rights that correspond to them as users against the company

sa service provider.

o In relation to this aspect, the LGTEL grants a specific nature

ca qualified to the rights of end users in this sector. Tie-

ne the consideration of "obligations of a public nature", according to

with what is indicated in Title III of the Law, whose Chapter V deals with the

end user rights.

o Likewise, the obligatory respect for the protection of personal data

of users in this sector (article 41 LGTEL) also appears within

inside the “obligations of a public nature” within the sector of the

electronic communications (Title III, Chapter IV).

The processing operations that are the subject of this file are related to

with the exercise of the rights that as end users of community services

electronic cations are being made by the operator's customers. In this sense, already

we have seen that the regulations of this sector confer a public nature both to the

provision of the service itself (“services of general interest”) and the specific regime

co protection of users (“obligations of a public nature”).

Within the specific rights of this sector, the regulatory regulation is

found in the Bill of Rights of the user of electronic communications services

case (Royal Decree 899/2009, of May 22). In its article 5 (Celebration of contra-

cough) the following is specified:

"two. Operators will not be able to access an end user's line without their consent.

express and unequivocal sentiment

It should be remembered that the facts prosecuted in this file have consisted

precisely in that, that is, in the improper issuance of SIM cards that

have allowed third parties outside the line to access it. It is therefore affected
the right of the end user that is considered a public obligation
co.
But not only that, but in attracting customers, and particularly in ex-
requesting SIM cards, it is necessary to comply with the provisions of Law 25/2007. This law
It is dictated in use of state competence in matters of public security, and has
in order to guarantee that the operators conserve and make available to the Forces
and Security Bodies, the data relating to the holders of community services
electronic calls and their traffic data. Article 2 establishes the following:
“They are recipients of the obligations related to the conservation of im-
established in this Law the operators that provide communications services
electronic devices available to the public or exploit public communications networks,
in the terms established in Law 32/2003, of November 3, General of
Telecommunications.”
Article 3 and, specifically for prepaid lines, the single additional provision,
establishes that all end users holding services must be identified
of electronic communications.
As has been proven in this file, the points of sale and centers of
answering telephone calls were used for the issuance of duplicates of
SIM cards. For these purposes, it would be applicable, in the identification of clients, the
mentioned Law 25/2007. This Law, at the time of its approval, was aware
of the possibility of using external entities in the processes of contracting
notwithstanding which, in any case, it established the operators as obligatory subjects.
gados. A possible failure in the identification by a distributor would be in all
case attributable to the operator.
Therefore, they are involved in the management of clients by the operators.

telecommunications carriers, aspects directly related to services

of general interest, obligations of a public nature and, above all, public security.

public of the State. This precludes considering that the service operator can be exonerated

electronic communications services from liability for the mere fact of having

outsourced its customer service channel services.

In this sense, in the provision of electronic communications services, the

operator would always have had the option of providing the service itself

customer service, instead of resorting to outsourcing techniques. The use of a

another option cannot cause liability to arise when they are involved.

two aspects of such a relevant nature.

For the rest, according to the documentation provided by TME, it is observed that in the

contracts it maintains with those in charge (both THADER and CATPHONE for a

hand, as with XXXXXX, on the other) is included (...).

Indeed, in (...), it is indicated:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

77/106

(...).

The same clause appears in the distribution contracts signed by TME with THA-

DER and CATPHONE.

Based on the foregoing, the allegation adduced must be dismissed and

TME is considered to be responsible for guaranteeing the security and confidentiality

of the personal data processed. Therefore, without prejudice to the obligations

established in other laws, the treatments carried out by TME must comply with the

data protection regulations.

3.2 RESPONSIBILITY OF THE BANKING ENTITIES

While these entities are responsible for processing the data of their

clients, they have the same obligations as those indicated up to now for the

operators referring to compliance with the RGPD and the LOPDGDD, and also the derivatives

of Royal Decree-Law 19/2018, of November 23, on payment services and other

urgent financial measures.

II. ON THE FOUNDATIONS OF LAW

FIRST. ON THE ALLEGED INFRINGEMENT THAT CONTINUES

BEING COMMITTED BY TME: VIOLATION OF THE

PRINCIPLE OF TYPICITY

It is true that the Agency recognized that “TME (…) in which the

way of acting of TME and those in charge” but also the fact that,

despite its existence, the infringement occurred.

1.1 ABOUT THE CONDUCT OF TME: IN NO CASE COULD IT CONSIDER

DERARSE SUBSUMABLE IN ARTICLE 5.1 F) RGPD.

The incardination of the facts in precept 5.1.f) RGPD, has been the subject of

analysis in the Third FD.

Regarding the infallibility alleged by TME, it should be noted that a

obligation of result, but of activity, but to evaluate said activity and

implementation of measures and their consideration as "adequate" is inevitable.

It is possible to analyze the methods used by the third party to illicitly access the

duplication process, the safeguards implemented by TME and the unavoidable-

mind, the result. These three elements are the ones that will determine the suitability

equation to risk and not as TME intends to focus the debate on whether it is infa-

ble or not your system.

The risk approach and the flexible risk model imposed by the GDPR -

starting from the double configuration of security as a relative principle

to the treatment and an obligation for the person in charge or the person in charge of the treatment.

in no case does it impose the infallibility of the measures, but rather their

constant equation to a risk, which, as in the case examined, is true

high, probable and not negligible, high and with a very significant impact on the

rights and freedoms of citizens.

1.2 ON THE DRAFTING OF THE REGULATION THAT RESULTS FROM APPLICATION

CATION: UNDETERMINED LEGAL CONCEPTS THAT CONTRIBUTE

YEN TO INCREASE THE LEGAL INSECURITY AND DEFENSE OF

TME.

It should be noted that, in the Law of the European Union (EU), the protection of

data has been recognized as a specific fundamental right. I will be-

taken in article 16 of the Treaty on the Functioning of the EU, as well as in

Article 8 of the EU Charter of Fundamental Rights. In view of

rapid technological advances, the EU adopted new legislation in 2016

to adapt data protection regulations to the digital age. The GDPR in-

entered into force in May 2018 and in article 4 it provides a series of “Definitions

tions” or certain legal concepts, among which are not included the

invoked by TME: adequate security, technical and organizational measures

appropriate or level of security appropriate to the risk.

Indeed, we are dealing with indeterminate legal concepts, concepts
abstract, which can only be concretized in its practical application. For
application of these concepts, the Agency has made a well-founded assessment
in technical criteria and logical reasoning developed in the FD that
support this Resolution and that, in that margin of appreciation, allow
foresee, with sufficient certainty, the sanctioned conduct.
Reference must be made to a precision made by the Constitutional Court
tional in Order 100/2001, of April 26:
According to the doctrine of this Court, the right to the principle of legality
of art. 25.1 CE, which includes the requirement of certainty in the prediction
termination of punishable conduct, is not incompatible with the use
tion by the legislator of indeterminate legal concepts, whose meaning
the latter has to be inferred by the interpreter through a systemic
theme of all the elements that make up the standard, taking into account the fi-
purpose and basis of the same (SSTC 69/1989, of April 20, FJ
1; 305/1993, of October 25, FJ 5; 26/1994, of January 27, FJ
4; 184/1995, of December 12, FJ 3). The language of the law is not so per-
effect that allows ruling out, in any case, imprecision or amphiboly.
Therefore, what art. 25.1 CE requires the legislator is that the conduct
written in the norm and object of sanction, is sufficiently recognizable
by their eventual recipients, and the applicator must reject all
those interpretations that clearly do not find coverage in the
same. On the contrary, when by means of an elementary logical inference
the interpreter can specify without difficulty the normative forecast, the pre-
sanctioning concept in question will comply with the requirements of typicity and
certainty required by art. 25.1 EC, although the sanctioned appellant -

as in this case - allege a different interpretation of the rule

in relation to the one carried out by the General Council of the Judiciary

in the exercise of its disciplinary power. In such cases, the control

purpose of this Court is to prevent the interpretation of the organ

punisher, protect applications of the rule in which it is projected

on behaviors that, according to their content, could not be foreseen and

reasonably fit into the type or illicit described by it.

1.3 SUBSIDIARILY: ON THE INTERPRETATION AND APPLICATION

OF THE REGULATION MADE BY THIS AGENCY. RISK OF VUL-

NERATION OF THE PRINCIPLE OF SPECIALTY.

In the instruction phase of the sanctioning file, the investigating body,

the concurrence of different types of offenders has already been considered, opting for

the application of article 83.5 of the RGPD, as it is a more serious infringement,

whose justification has been clarified in the Third FD.

It should be noted that the 2021 Report of the State Attorney General's Office

dedicated to "Computer Crime" dedicates in its point 8 a mention

tion to fraudulent actions online:

“In this brief review of online fraudulent actions, it is obligatory

Mention is made of the behaviors that affect the telecommunications sector.

cations in their different variants, and closely related to them, although

the damage is generated in online banking, commonly known as

SIM Swapping fraud, which is being used with alarming frequency
in recent years. The technique consists of circumventing the security measures
identity of banking entities by accessing the alphanumeric codes
of confirmation, of unique use, generated on the occasion of the transactions
electronic forms and that are ordinarily communicated to clients through
through SMS messages. To do this, criminals obtain prior
mind a duplicate or a new SIM card in the name of your victim, since
be requesting it from the corresponding operator, simulating the identity of
that, either using a more elaborate methodology, as in
the supposed object of judicial investigation in Zamora, in which
chaba for that purpose a mobile repair shop.
Once they have the SIM card at their disposal, criminals are guaranteed
they certify the reception in their own device of the confirmation code of
the fraudulent transaction and, ultimately, the possibility of making effective
the same for your benefit, preventing it from being known at that time
for the injured party. This form of fraud has generated
In recent years, multiple police investigations and the initiation
of legal proceedings in different territories such as A Coruña and Va-
lence. Their effectiveness and the ease with which criminals achieve their
illicit purposes has determined the adoption by telephone operators
phony of specific measures of prevention and strengthening of the ga-
guarantees for the issuance of these cards or their duplicates."
The disputed facts are considered to be of sufficient relevance and
gravity, so as to, in application of the specialty principle, subsume
milos in a violation of article 5.1.f) of the RGPD, precisely, because
that the security of customer data has not been guaranteed -for-

adequate-, and consequently, a non-autonomous treatment has been produced.

unauthorized and illegal that affects the confidentiality of data and that has become

in other consequences, not at all trivial, such as the economic damages

which would not have occurred if TME had ensured the identity

identity and correct authentication of its clients.

SECOND. ON THE CLASSIFICATION OF THE ALLEGED CONDUCT IN

OTHER SANCTIONING PROCEDURES INITIATED AGAINST TME AND TE-

LEFÓNICA DE ESPAÑA, S.A.U (TDE): ERROR IN THE RATING OF

THE INFRINGEMENT.

In the Third FD we have already clarified that it is not an error in the qualification

of the infraction but of an interpretation that, by reason of the facts,

Guys, the Agency qualifies it that way.

It is article 27 of the LRJSP under the heading of "Principle of typicity",

the one that has:

1. Only the violations of the organ-

legal order provided as such infractions by a Law, without

prejudice to the provisions for the Local Administration in Title XI of the

Law 7/1985, of April 2.

Administrative infractions will be classified by law as minor, major,

you see and very serious.

2. Only for the commission of administrative infractions may im-

impose sanctions that, in any case, will be delimited by the Law.

Integrating the facts in articles 83.5.a) of the RGPD and 72.1.a) of the

LOPDGDD, the regulatory predetermination requirements are met

and certainty that derive from the principles of legality and legal certainty.

ca (articles 9.3 and 25 EC).

THIRD. THE CONDUCT OF TME IS NOT UNLAWFUL

The violation of the imputed administrative infraction responds to a

concept included within "Principles related to treatment" that requires a

adequate security in the processing of personal data, security

that has not been guaranteed according to the Proven Facts.

Illegality is the quality that has a previously typical behavior

of violating the legal system and the purposes it pursues. of this

Thus, in order to be punishable, it is not enough that the conduct

je in the description contained in the type, but with this they are vulne-

achieving the objectives pursued by law. In this regard, the conduct

will be unlawful if the legal interest protected by the violated precept is damaged.

rare.

In this case, the legislation on the protection of personal data

follows the purpose that those responsible and in charge of the data

They treat them by having security measures

that prevent the illicit or fraudulent use of the same. And this legal good

has been injured in the events that are the subject of this proceeding.

According to STC 246/1991 "(...) this different construction of imputability

of the authorship of the infraction to the legal person arises from the very nature

law of legal fiction to which these subjects respond. missing in them

volitional element in the strict sense, but not the ability to violate the

rules to which they are subject.

Capacity for infringement and, therefore, direct blame that derives from the

legal right protected by the norm that is violated and the need for

said protection is really effective and because of the risk that, consequently,

cia, must assume the legal entity that is subject to compliance with di-

cha norma" (in this sense STS of November 24, 2011, Rec

258/2009).

Therefore, the allegation is dismissed. The ultimate responsibility rests

about the treatment continues to be attributed to the person in charge of the treatment,

who is the one who determines the existence of the treatment and its purpose. Record-

We give that, in general, the operators treat the data of their

customers under the provisions of article 6.1 b) of the RGPD, therefore

be considered a necessary treatment for the execution of a contract in the

that the interested party is a party (...).

QUARTER. NO FAULT

It alludes to the professional diligence with which he has acted.

Regarding the behavior of MSD, it is considered that it responds to the type of infraction

tor and to the title of guilt. TME is considered to have acted negligently.

As a repository of personal data on a large scale, therefore,

accustomed or dedicated specifically to the management of personal data

clients' staff, you must be especially diligent and careful in

your treatment. In other words, from the point of view of guilt, we are before

a defeatable error, since with the application of technical and organizational measures

adequate organizational measures, these identity thefts could have been

avoid.

Thus, the infraction occurred not because of the lack of a specific privacy policy.

security for the issuance of SIM duplicates, but because of the need to

their revision and reinforcement.

It is not enough to have a security policy, but it is also necessary to

quarla to mitigate the risks. The continuous advancement of technology and

evolution of the treatments propitiate the continuous appearance of new

risks that must be managed. In this context, the GDPR requires that

data controllers implement adequate control measures

to demonstrate that the rights and freedoms of persons are guaranteed.

people and data security, taking into account, among others, the “risks

risks of varying probability and severity for the rights and freedoms of

natural persons” (article 24.1) applying the appropriate measures.

Certainly, the principle of responsibility set forth in article 28 of the

LRJSP, provides that: "They can only be sanctioned for constitutive acts

natural and legal persons, as well as,

when a law recognizes their capacity to act, the affected groups

two, the unions and entities without legal personality and the in-

dependent or self-employed, who are responsible for them to you.

title of fraud or fault."

However, the mode of attribution of responsibility to legal persons

dicas does not correspond to the forms of fraudulent or reckless guilt

that are attributable to human behavior. So, in the

case of infractions committed by legal persons, although it must be

concurrence of the element of guilt, it is necessarily applied in

way different from how it is done with respect to natural persons.

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 culpability of the conduct must also be proven, must

be considered in order to assume the corresponding load, which

the volitional and cognitive elements necessary to learn

ciate that they are part of the typical behavior tested, and that their exclusion

requires that the absence of such elements be proven, or in its aspect

regulations, that the diligence that was required by whoever

alleges its non-existence; not enough, in short, for exculpation in the face of a

typically unlawful behavior the invocation of the absence of

fault".

In the case of complaining party one, an attempted duplication occurs.

do corresponding to the telephone number ***TELEPHONE.2, on date 5

February 2019, which fortunately did not bear fruit in the delivery to the

supplanting person. However, and despite the fact that he changed his number

phone number ***PHONE.1, is again affected by a second in-

Attempt, a month later -on March 6, 2019-, what an unfortunate-

cially, it does materialize and is delivered to the supplanted person.

dora, running out of line and consequently losing control of

your personal information. Let us remember that it is the affected person who

declares to receive a notice by means of a telephone call from ***PRO-

VINCIA.2 of a possible impersonation attempt. We also highlight

the existence of an email written by TME staff, of

dated March 7, 2019, in which it is recognized that who issues the certificate

second duplicate, (...). To this must be added, residence in ***LOCA-

LIDAD.4, province of Barcelona of the affected party, and (...) located in ***LO-

CALIDAD.2 (***PROVINCIA.2) and the issuance of the second duplicate in

(...) the city of ***PROVINCE.1.

As for the complaining party two, the duplicate is issued (...) in

***LOCATION.4 (Barcelona) when the affected party has his domicile in

Las Rosas (Madrid).

(...).

In the case of claimant three, there is (...), which becomes

the issuance of a duplicate of the line ***TELÉFONO.5, even if there is

contacted TME thirteen minutes after receiving the email.

co that confirms the withdrawal from Movistar Cloud. Also, it has been possible

check that in the recording of the change of ownership of the service

provided by the affected party, (...). We would not, therefore, be faced with a deception.

of a third party, but in the presence of security measures

which then manifested themselves as insufficient, became inappropriate.

das and did not guarantee an adequate level of security in the process of

verification of the identity of applicants for a change of service.

Given this, we must insist that the safety of a procedure is,

like that of a chain, that of its weakest link, and in the case of this

establish strict security measures in a channel, if they are not established

also equivalent measurements in the rest of the channels, it is reducing

ceding global security to that of the minor security channel.

4.1 DILIGENT ACTION, GOOD FAITH AND LEGITIMATE TRUST

OF MSD

He adduces how striking it is that, in the Motion for a Resolution, for a

On the other hand, certain affirmations are indicated that include positive evaluations and

on the other hand, others are indicated in the opposite direction.

It is true that as an operator it is subject to the “Obligations of public service”.

public and rights and obligations of a public nature in the exploitation of networks

and in the provision of electronic communications services” of the LGTEL.

However, TME cannot deny the fact that it processes data of a personal nature.

large-scale sound. It is the operator itself that acknowledges having more than

eight million customers.

Indeed, in sanctioning matters the principle of culpability (STC

15/1999, of July 4; 76/1990, of April 26; and 246/1991, of December 19

bre), which means that there must be some kind of fraud or guilt. What

says the STS of January 23, 1998, "...one can speak of a determined lí-

jurisprudential line that rejects in the sanctioning scope of the Administration

strict liability, requiring the concurrence of fraud or negligence,

in line with the interpretation of the STC 76/1990, of April 26, when pointing out

that the principle of culpability can be inferred from the principles of legality and

prohibition of excess (article 25 of the Constitution) or the demands

inherent in the rule of law".

The lack of diligence when implementing safety measures at origin

Proper authority constitutes the element of guilt.

4.2 DUE DILIGENCE IN THE CHOICE AND SUPERVISION OF THE

CHARGED OF THE TREATMENT AND RESPONSIBILITY OF THIS:

It also appeals to the existence of exceptional circumstances and beyond

TME and the due diligence shown, since it cannot be considered

responsible for exceptional breaches of the operations carried out

carried out by those in charge of the treatment. This claim must be

dismissed because the signed contracts already provide that the treatments

those made by those in charge will be made on behalf of the person in charge, that is,

that is, TME (article 29 RGPD).

From TME's statements the conclusion seems to be drawn that it has no

no power of action to prevent these frauds or impersonations, since

attributes all responsibility to intervening third parties (managers or su-

planters). We do not agree with this conviction. Also po-

We could refute the inconsistency of these affirmations because, for a

side, cites due diligence in their selection and supervision, invokes the STS

1232/2018 to confirm that it has fulfilled the surveillance duties, and

on the other, it holds them responsible for the facts.

Also, the fact that the Agency has recognized that there are certain

clauses that define the terms of the relationships with those in charge of the

treatment, does not exempt you from risk management, which is one of the pillars of

the leadership of any organization. Every entity, when it intends to lend

with guarantees a service, must manage the elements of uncertainty that

are derived from its nature, scope, context and purposes.

The concepts of controller and processor are not formal,

but functional and must attend to the specific case. The person responsible for the treatment

treatment is from the moment it decides the ends and means of the treatment.

without losing such condition the fact of leaving a certain margin of action

tion to the person in charge of the treatment. This is unquestionably expressed in the Di-

CEPD guidelines 07/2020 -the translation is ours-:

“A data controller is the one who determines the purposes and

the means of treatment, that is, the why and how of the treatment.

I lie. The data controller must decide on both

purposes and means. However, some more practical aspects

of implementation ("non-essential media") can be left in

hands of the treatment manager. It is not necessary that the res-

responsible actually has access to the data being processed

to qualify as responsible.

Likewise, in point 6 it is said (the translation is ours):

The data controller will be responsible for compliance with

the principles established in article 5, paragraph 1, of the RGPD; Y

it's

The data controller must be able to demonstrate compliance

observance of the principles established in article 5, paragraph 1, of the

GDPR

Also in point 8 they establish:

The principle of liability has been further developed

in article 24, which establishes that the controller of the traffic-

will apply the appropriate technical and organizational measures to

guarantee and be able to demonstrate that the treatment is carried out in accordance

mited with the RGPD. These measures will be reviewed and updated in

necessary case. (…)

4.3 EXCEPTIONAL CIRCUMSTANCES AND OUTSIDE TELEFÓNICA:

• Possible negligence in the care of personal data on the part of

users: the users themselves have the responsibility of custodian

properly disclose your personal data.

The Internet Security Office tells us that the “Duplicate card

SIM or SIM card exchange -SIM Swapping-” “is based on the duplication

of our SIM card, and for this, the attackers need some personal data.

such as name and surname, DNI, date of birth, the last 4 days

payments from our bank account, etc., that they have been able to obtain by other means,

such as phishing or buying in online stores

. With these da-

cough, the attackers request a duplicate of our SIM, supplanting our

identity with the above data before the operator. Meanwhile, the only thing

we notice is that our device runs out of mobile coverage, and when

we connect to a Wi-Fi network, we will begin to receive notifications of mo-

movements made from our mobile without our consent, such as

bank transfers or online purchases, among others".

fraudulent

It is true that it is outside the scope of responsibility of TME the information

personal information that can be shared by those affected. what is inside

its sphere of control is the definition of the procedures, systems, controls

rules and security measures applicable depending on the criticality of the treatment.

that ensure the correct identification of the holder of the line.

• Probable liability of third parties unrelated to TME, such as entities

banking entities that have operated in each case

Certainly, the PSD2 Directive applies to payment services provided

within the Union (article 2), and not to TME, but it is also true that the ex-

Request for a duplicate SIM card in favor of a third party who is not the owner.

The line manager gives spoofers control of the phone line.

ca, and therefore, of the SMS addressed to the phone linked to the SIM card

initial and in this way to be able to access to know the authentication code

tion of the transaction.

Pursuant to article 4.30 of the Directive, "strong authentication" is based on

in the use of two or more elements categorized as knowledge

(something only the user knows about), possession (something only the user owns), and

inherence (something that is the user). These elements or factors are independent

teeth against each other and, therefore, the violation of one does not compromise the reliability

of others.

The foundation is very simple: the more elements you have to verify,

identify the user's identity, the more secure the transaction.

Let us remember that, in these cases, the impersonator must first, in-

Enter the username and password or password in the application or on the website

payment service provider or online banking. Second, for

complete the transaction or electronic management that you wish to carry out, the supplanting

The customer will receive, normally through an SMS, an alphanumeric code of the

verification on the mobile phone linked to that profile. This code has a

limited temporary validity and it is of a single use, that is to say, it is only generated

for that specific transaction and for a limited time. Once you enter

Once the verification code was given, the transaction would go through and complete. I know

assumes that only the user has the mobile device in his possession (it would be the

“something you have”), so when receiving the verification code on said mobile phone,

fication via SMS, your identity would be doubly authenticated. By

Therefore, it would not be enough for the impersonators to be able to commit the fraud with

know the username and password with which the victim identifies, but

it will be necessary for them to intercept said confirmation code. Consequently,

in order to carry out a non-consensual transfer, transaction or purchase.

that is, to carry out the computer fraud, the cybercriminal must

will illegitimately access the verification codes associated with each

of these operations sent by the bank through SMS and the

The most common way to do this is by obtaining a duplicate

of the SIM card.

Therefore, it is necessary to execute two completely different actions

but complementary to each other.

First of all, you must obtain the access data for online banking or

payment provider owned by the person to be defrauded, if we focus on

the search for wealth enrichment.

And secondly, it will be necessary to obtain the duplicate of the SIM card owned by the

identity of the person to defraud in order to get hold of the SMS of

confirmation that the client will receive on his mobile terminal as authentication

double factor.

Well, in the last of these actions -obtaining the duplicate-, it is where

the facts that are the object of this procedure have been focused and not on the events

decided in the first phase, who remain outside the responsibility that is

imputes to TME.

• Intentional actions of third parties to commit a crime

Regarding TME's lack of responsibility, it should be noted that, with

general character TME treats the data of its clients under the provisions of

Article 6.1 b) of the RGPD, as it is considered a necessary treatment for the

execution of a contract in which the interested party is a party or for the application

at the request of the latter of pre-contractual measures. In other cases, substantiate

the legality of the treatment on the bases provided for in article 6.1.a) and f) of the

GDPR.

It is true that, to complete the scam, it is necessary for a third party to “impersonate the identity” of the owner of the data, to receive the duplicate of the SIM card.

What entails a priori, a treatment outside the principle of legality because a third party is treating data, since it has access to them, without legal basis alguna, in addition to the violation of other principles such as confidentiality dad.

For this reason, this is a process in which the diligence provided by the operators is essential to avoid this type of scams and violations of the GDPR. Diligence that translates into the establishment of adequate measures to ensure that data processing is in accordance with the RGPD.

Regarding the fact that the commercial agents of the face-to-face and telephone channel have been deceived and induced to commit human errors when applying identification operation designed, it should be noted that TME must be in disposition to establish mechanisms that prevent duplication fraudulent cation of SIM cards, measures that respect the integrity and confidentiality of the data and that prevent a third party from accessing data that are not owned by them, since it is precisely the operator's responsibility to treat personal data in accordance with the RGPD (recitals 76, 77, 78, 79, 81 and 83 GDPR; article 32 of the RGPD and article 28 of the LOPDGDD)

We have already consigned in the Proven Facts, the existence of the contracts and applicable clauses. However, TME cannot evade responsibility that corresponds to it regarding the security of the treatment, hiding behind the existence of contractual clauses that it claims have been breached by

part of the managers. Let us remember that in all three cases, those in charge

act on behalf of TME, in the case of (...).

To improve policy compliance by dealers

the instructions that are shown to them must be clear, being recommendable

the inclusion of these in the information system, within the process of change

SIM bio, even with controls on system screens such as buttons

acceptance tones that prevent the continuity of the process if it is not accepted

have performed a certain action.

Periodic testing, measurement and evaluation of the effectiveness of

technical and organizational measures to guarantee the security of the treatment

are the responsibility of each controller and processor in accordance with

me to article 32.1.d) of the RGPD.

Therefore, TME as data controller is obliged to verify

both the selection and the level of effectiveness of the technical means used

two. The completeness of this verification must be evaluated through the prism

risk adequacy and proportionality in relation to the state

of technical knowledge, implementation costs and the nature, al-

scope, context and purposes of the treatment.

The concurrence of force majeure is not appreciated. As indicated by the in-

tructora in the Resolution Proposal, in the cases described in the section

of proven facts, data security was not effectively guaranteed.

tive, and in particular, its correct custody to avoid loss, theft or

Unauthorized access.

FIFTH. BREACH OF THE PRINCIPLE OF PROPORTIONALITY

Regarding the breach of the principle of proportionality, the RGPD provides

expressly the possibility of graduation, through the provision of fines

susceptible 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

variables that have been analyzed by this Agency, to which it is necessary to submit

check the graduation criteria provided for in the LOPDGDD, object of development

llo in the FD Seventh.

It should be noted that the agreed administrative fine will be effective because

will lead the company to apply the technical and organizational measures that

guarantee a degree of safety corresponding to the criticality value of the

treatment.

It is also proportional to the violation identified, in particular its degree.

truth, the risks that have been incurred and the financial situation of

the company.

And finally, it is dissuasive. A dissuasive fine is one that has a

genuine deterrent effect. In this regard, the Judgment of the CJEU, of 13

June 2013, Versalis 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: 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»);

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 three claims presented.
through which it can be verified that, from the moment in which the loss
impersonating sona performs the SIM replacement, the victim's phone remains

without 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 fact, the complaining party two denounces that: “In my case, the thief took the

calls made to my phone number. I myself, I got to talk to him.”

In short, they may supplant the identity of those affected, being able to access and

control, for example: email accounts; bank accounts; Applications

like WhatsApp; social networks, such as Facebook or Twitter, and much more. In short-

give accounts, once the access code has been modified by the impersonators

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 TME duplicates 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 (claimant party three), after overcoming by the

people impersonating the security policies implemented by the operator, which

that evidences a breach of the duty to protect customer information.

This unauthorized access to the personal data of those affected is determined

te for subsequent actions carried out by the impersonators, since

that take advantage of the space of time that elapses until the user detects the fac-

llo on the line, he contacts the operator, and she detects the problem, to

carry out fraudulent banking operations -which have been reproduced in the three cases

denounced - and that without the duplication of the SIM card it would have become impossible to

realization.

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

whereby TME has 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.

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, prior assessment of the allegations adduced

for the purposes of a correct application of the principle of proportionality.

On the one hand, the following aggravating factors have been taken into account:

- Article 83.2.a) RGPD:

The nature, seriousness and duration of the offence, taking into account

the nature, scope or purpose of the processing operation that

concerned, as well as the number of stakeholders affected and the level of

damages that they have suffered:

It is not that the AEPD has valued differently the different cir-

concurrent circumstances of the precept, but opted for an assessment

independently so that the analysis of each one would be clearer.

However, nothing prevents a joint analysis which is as follows:

The violation of the principle of article 5.1.f) RGPD entails an im-

important for the rights of those affected. The Agency considers that

the nature of the infraction is very serious since it entails a loss

loss of disposal and control over personal data. has allowed

criminals steal identity by hijacking phone number

phone number after obtaining a duplicate of your SIM card. Behind the

entry into force of the PSD2 Directive, the mobile phone has become

play a very important role in making online payments by being

necessary for the confirmation of transactions, and converts this dis-

positive -and by extension to the SIM card-, in clear objective of the cyber-

criminals.

It refers to SAN 496/2017, although we consider that the circumstances

referred to are different. In that case, a violation

neration of article 77.37 of the LGTEL. The Court considered that the

Non-compliance or incorrect fulfillment of the obligation, in the processing

casualties, did not cause a serious violation of the rights

of consumers and end users, which is why it turned out to be more favorable

rable the qualification of the infraction as minor.

In relation to the time period with respect to which the events occurred,

although the facts denounced by the complaining parties occur

on certain dates, TME declared in fiscal year 2019 for the mar-

ca Movistar a total of XXX cases and in the previous actions of in-

investigation provided a list of XX cases ranging from January 14

2020 until June 12, 2020. Therefore, the application as

mitigating factor of article 76.2.a) of the LOPDGDD - continued nature of

infringement - as TME states, is incompatible with the appraisal of the

duration of the offense as an aggravating circumstance, which, maintaining

mos as such.

The percentage of fraudulent SIM card applications declared by

TME in fiscal year 2019 amounts to X,XXXXX % with respect to the total of

SIM card changes managed: XXXXXXX changes.

The percentage of fraudulent SIM card applications declared by

TME until the month of June 2020 amounts to X.XXXXX % with respect to the

total SIM card changes managed: XXXXXX changes.

Specifically, for the Movistar brand, the figure corresponding to 2019

(XXX cases) is broken down as follows:

(...).

The cases detected and notified to the Agency up to the month of June

of 2020 amount to XX cases.

And although there have been three reported cases, the previous actions

of investigation identified the existence of other cases (TME declared

for the Movistar brand in 2019 a total of XXX cases and

provided a list of XX cases ranging from 01/14/2020 to

06/12/2020).

In relation to the level of damages and losses suffered, the Agency

considered high, since it has led to fraudulent banking operations

tas occurred in a short space of time. Through duplication

of SIM cards, alleged impersonators have managed to control

control of the subscriber's line and specifically the reception of targeted SMS

to the legitimate subscriber to carry out online operations with entities

banks impersonating his personality. These SMS are sent by entities

bank details as part of the two-step verification of transactions

tions such as money transfers or Internet payments, and the access

so to these SMS is usually the reason for the fraudulent duplication of the

SIM cards.

It is true that TME is not responsible for identification policies

of clients established by banking entities nor can it be attributed

bury the responsibility for bank e raud. However, it is also

true, that if TME 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. this sequence

of facts revealed in the claims filed ge-

would be a series of serious damages that should have been

taken into account in an impact assessment relating to the protection of

data (considering 89, 90, 91 and article 35 of the RGPD). Definitely,

from the moment a duplicate is delivered to a person other than

the owner of the line or authorized person, the customer loses control of

the line and the risks, damages, multiply. In addition, I have

Many happen with overwhelming immediacy.

In short, the application of the aggravating circumstance of article 83.2.a) of the RGPD is

refers to all these previously analyzed aspects, positions of

manifest in the Proven Facts, in the social alarm generated by the

carrying out these fraudulent practices and due to the very high probability

materialization of the risk, without determining the number of re-

claims filed. 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 re-

claims filed with the AEPD.

- Article 83.2.b) RGPD:

Intentionality or negligence in the infringement:

It alleges that the events that occurred with the three claimants

they cannot be considered in any way as a sample

representative of the level of commitment shown by TME in

compliance with its obligations regarding the protection of

data and, much less, the degree of effectiveness of some

security policies that are designed to serve a

volume of clients that exceeds 8 million and that the percentage

je of fraudulent applications is minimal.

Although the Agency considers that there was no intention to

part of TME, concludes that it was negligent in failing to secure a

procedure that guarantees the protection of personal data

end of customers. So, a result

socially harmful that imposes the disapproval of the policy

implemented security system that was ineffective, independently

of the level of commitment shown, which is unquestionable.

feasible.

Deny the concurrence of negligent action on the part of

TME would be equivalent to acknowledging that their conduct -by action or omission-

sion- has been diligent. Obviously, we do not share this

perspective of the facts, since it has been accredited the

lack of due diligence. A large company that treats

processing of personal data of its customers on a large scale,

systematically and continuously, you must take extreme care in the

compliance with its obligations regarding the protection of

data, as established by case law. It is very illus-

the SAN of October 17, 2007 (rec. 63/2006), based on

that they are entities whose activity involves

in continuous processing of customer data, indicates that "... the

The Supreme Court has understood that there is imprudence

whenever a statutory duty of care is disregarded, i.e.

when the offender does not behave with due diligence. Y

in assessing the degree of diligence, special consideration must be given to

especially the professionalism or not of the subject, and there is no doubt

that, in the case now examined, when the activity of the re-

current is of constant and abundant management of data of ca-

personal character

must insist on rigor and exquisite care

for complying with the legal provisions in this regard".

The risk analysis of the treatment is established as fundamental.

processing of data according to the specific circumstances of the

operator, such as volume and type of data. It is vital

importance of establishing and implementing procedures and measures

necessary, depending on the characteristics and entity of this,

to demonstrate that due diligence has been carried out

when trying to prevent an impersonation of

identity. Thus, even if the damage was done by a third party,

zero external to the company, it must be possible to demonstrate that

taken the necessary precautions during the development of

business activity, required by the regulations, to avoid a

damage that was foreseeable. It's about having a level of care

objective taking into account the specific circumstances of the case that

make it possible to make it clear that he was aware of the possibility

of suffering an identity theft, and that, with it, is applied

appropriate measures were taken to reduce the materialization of such

risk to the minimum possible.

- Article 83.2.d) RGPD:

 Degree of responsibility of the data controller or data processor

taking into account the technical or organizational measures that

have applied under Articles 25 and 32:

He claims not to understand the conclusion of the Agency that qualifies the

degree of responsibility as high.

Responsibility for vulnerabilities in the procedure

for the issuance of the duplicate SIM card corresponds to

TME.

Those in charge of the treatment -distributors and suppliers-

res, where appropriate - they only process the data following the instructions

documented by the person in charge and contractually defined

give the consequences of its non-compliance.

The personal data that TME collects both for contracting

of the service as during its provision, are your responsibility.

and must be treated in a way that allows good development

development of the contractual relationship between the parties, guaranteeing in

at all times the application of the principles of article 5

GDPR. And this is independent of whether the treatment is carried out

by himself or through a treatment manager.

In this sense, article 28.3.h) of the GDPR establishes

continuous supervision by the person in charge of the

treatment by indicating that the person in charge "will make available to the

responsible for all the information necessary to demonstrate the

compliance with the obligations established in this article

article, as well as to allow and contribute to the realization of autho-

audits, including inspections, by the person in charge or

another auditor authorized by said person in charge.

Regarding the performance of audits as an appropriate means

for the data controller to monitor

continues to the person in charge of the treatment, the Guidelines 07/2020

of the CEPD establish that: “99. The obligation to use

only to data processors "who provide

sufficient guarantees" contained in article 28, paragraph 1,

of the GDPR is an ongoing obligation. does not end in

time when the controller and the data processor

enter into a contract or other legal act. Instead, the controller

should, at appropriate intervals, verify the warranties of the

processor, including through audits and inspections when

proceed". (The translation is ours).

The Agency considers that TME has mitigated the risks as a result of

the investigation initiated and has increased the security measures

authority in order to guarantee the identity of the client. He has

submitted documentation to determine with certainty the mo-

moment in which the measures have been taken once produced

the facts.

Therefore, you are responsible for not having done everything you

could be expected to do, given the nature,

purposes or scope of the processing operation, in light of the

obligations imposed by the GDPR.

- Article 83.2.e) RGPD:

 Any previous infringement committed by the data controller:

It adduces MSDs that do not refer to the same type of offender.

The allegation adduced is upheld, in part, and it is only considered

infractions prior to the Agreement are considered as aggravating

Startup actions committed by TME, which are considered pertinent or

relevant.

It should be noted that recital 148 of the GDPR adds that

must refer to “any relevant prior violations” or “relevant

vante” of the translation of the original text in English “relevant”.

For this reason, we only consider the two procedures in which

sanctioned to TME (firm resolutions in administrative proceedings)

consequence of treatment without legitimacy for fraud of

identity.

Procedure No.

I lie

Resolution date

sanctioned

dora

Infraction imputed

gives

Sanction

PS/00453/2019

Fraudulent contracting of telephone lines without the consent of the person

affected.

03/18/2020

6.1. GDPR

40,000.00

PS/00235/2020

01/21/2021

6.1.GDPR

75,000.00

There is a change of ownership of the line in favor of a third party, without

had carried out any type of identity verification in this regard.

- Article 83.2.g) RGPD:

 Categories of personal data affected by the breach:

The personal data affected by the treatment has a

particularly sensitive as it enables identity theft.

ty.

The delivery of a duplicate SIM in favor of a different third party

of the legitimate owner is considered particularly serious since

enables the sending or receiving of calls, SMS, or access to the

data service, which becomes in the hands of the person

planter.

Once the duplicate is obtained, the path to the applications is opened.

tions and services that have as a recovery procedure

password sending an SMS with a code to be able to change

the passwords. In short, it enables identity theft

dad.

And although they have not been affected "Special categories of

personal data" as defined by the RGPD in article 9, this does not

means that the stolen data was not of a sensitive nature.

ble. It is not about the personal data that is required for the expedi-

tion of the duplicate of the card, if not of the card itself as

personal data associated with a telephone line owner of a

user, which is obtained with the purpose of supplanting your identity

to obtain access -among others- to banking applications or

electronic commerce, in order to interact and carry out

operations on your behalf, authenticating through a user

and password previously taken from that user, as well as

with double factor authentication when receiving the confirmation SMS

mation on your own mobile terminal where you will have the tar-

duplicate SIM card.

~

Article 76.2.b) LOPDGDD:

 Linking the activity of the offender with the performance of treatment

Personal data processing:

C/ Jorge Juan, 6

28001 – Madrid

The development of the business activity carried out by TME

www.aepd.es

sedeagpd.gob.es

requires continuous and large-scale processing of data

customers' personal data, according to the number of telephone lines

mobile voice company reported in the "EIGHTH Background", which

positions TME as one of the telecommunications operators

largest tions in our country. Not applicable, as claimed

of TME, its application as a mitigating factor.

On the other hand, the following mitigating factors are taken into consideration:

- Article 83.2.c) RGPD:

 Measures taken by the person responsible to mitigate the damages and losses

damages suffered by the interested parties:

Positive, considering the complexity of implementing

New measures.

Namely:

(...).

Article 83.2.f) GDPR:

 Degree of cooperation with the supervisory authority:

Tall. The Agency considers that TME has cooperated fa-

vorable with research, providing answers to the ma-

majority of the requirements and forming part of the GT.

- Article 76.2.c) LOPDGDD:

 The benefits obtained as a result of the commission of the investment

fraction.

This Agency does not consider that TME has obtained a benefit

beyond receiving the cost price set for the

issuance of duplicate SIM cards.

- Article 76.2.h) LOPDGDD:

 Submission to conflict resolution mechanisms.

Various telecommunications operators, including

finds TME, signed with AUTOCONTROL a Protocol

that, without prejudice to the powers of the AEPD, pre-

sees mechanisms for the private resolution of controversies

tives to data protection in the field of contracting and

advertising of electronic communications services, dated

September 15, 2017. Protocol whose effective application

should be considered mitigating.

The allegations adduced in relation to the following attenuations are upheld-

you, which are taken into account:

- Article 83.2. j) GDPR:

Regarding adherence to approved certification mechanisms,

in accordance with article 42. TME has a System of

Management of Criminal Compliance accredited in accordance with the

UNE 19601 standard.

The arguments adduced in relation to the mitigating factor are rejected

provided for in article 83.2.k) of the RGPD. TME does not prove the existence of

the economic losses suffered. The complexity of implementing new

measures, as well as the audit of the Organization and Management Model for

Crime Prevention has been assessed through the attention

Nuant provided for in article 83.2.c) RGPD. Finally, the attendance of

obligations derived from the applicable regulations operates both against persons

physical and legal entities.

Likewise, and following the criteria expressed by the SAN, Chamber of the Contents

cioso-administrative, Section 1, Judgment of May 5. 2021, Rec.

1437/2020, finally the provision in the

article 76.2.a) LOPDGDD, regarding the continuing nature of the infringement,

that does not attend According to this sentence: “Consider, on the other hand, that

the non-commission of a previous infringement should be considered as a mitigating factor.

Well, article 83.2 of the RGPD establishes that it must be taken into account

for the imposition of the administrative fine, among others, the circumstance

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

treatment". This is an aggravating circumstance, the fact that

concurrence of the budget for its application implies that it cannot be all

taken into consideration, but does not imply or allow, as the act intends,

ra, its application as a mitigating factor”.

The allegation regarding the application of article

76.2.d) LOPDGDD: “The possibility that the conduct of the affected person had

could have induced the commission of the offence”.

TME has argued that the duplicates would not have been possible if the impersonator

dor had not carried out a previous illegitimate capture of the personal data

nals of said clients.

Well, the precept connects the conduct of the affected party with the commission of

an infringement: the possibility that the conduct of the interested party induces the

commission of the specific infraction imputed to the defendant by the

AEPD. Let us remember that TME is charged with the infringement of art. 5.1.f) of the

GDPR; fraud is not imputed to him, nor the treatment of data without legitimacy,

but a lack of guarantees of security measures that produces a

transfer of data to a third party.

Thus, in the case now examined, the infringement charged for lack of income

guarantees of security measures is an obligation imposed by the or-

legal order to the person in charge of the treatment, of which it is integral

responsible mind, in such a way that the conduct of the interested party (in his

case, supply by deception, carelessness or voluntarily your data to the third party.

zero that supplants it, since it must be considered that, in this case, the third

may have obtained the data without the intervention of the affected party) is independent

pending the deficient establishment, maintenance or control of the

security measures set by the data controller. The infringement

tion is unrelated to the action of the interested party and nothing that the latter does

mo would influence your commission.

On the other hand, it is considered that the precept focuses on behavior only

of the interested party and not of a third party interposed between the interested party and that

who commits the offence. That is, it seems that it directly links an action

tion or omission of the interested party with that induction. The performance of a third

ro, in what we could call a second phase -after a first of

obtaining the data-, against the person responsible for the treatment and the conduct

of the third party regarding the induction of the commission of the infraction, exceeding

area of action of the affected party. The interested party does not control what

does the third party with your data or the behavior of the third party. In addition, the

legislator has mentioned only the affected party and not a third party literally

of the precept.

In the exposed case, given that the person who has acted in front of the operator is

a third party and not the interested party, the precise assumption of fact would not occur

to apply this fader. It is the conduct of the third party (a criminal) that

posing as the interested party induces the controller to act self-

creating a duplicate SIM card.

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,

RESOLVES:

FIRST: IMPOSE TELEFÓNICA MÓVILES ESPAÑA, S.A.U., with CIF

A78923125, for an infringement of article 5.1.f) of the RGPD, typified in article

83.5.a) of the RGPD and classified as very serious for prescription purposes in the article

72.1.a) of the LOPDGDD, an administrative fine amounting to 900,000'00 euros

(nine hundred thousand euros).

SECOND: NOTIFY this resolution to TELEFÓNICA MÓVILES ESPAÑA,

S.A.U.

THIRD: Warn the sanctioned party that she must enforce the sanction imposed

Once this resolution is enforceable, in accordance with the provisions of

article 98.1.b) of the LPACAP, within the voluntary payment term established in article

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,

December, through its entry, indicating the NIF of the penalized person and the number of

proceeding that appears in the heading of this document, in the restricted account

nº ES00 0000 0000 0000 0000 0000, opened in the name of the AEPD in the bank

caria CAIXABANK, S.A. Otherwise, it will proceed to its collection in period

executive.

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 article 16.4 of the LPACAP. You must also transfer to the

Agency the documentation that proves the effective filing of the contentious appeal

so-administrative. If the Agency was not aware of the filing of the appeal

contentious-administrative within a period of two months from the day following the notification

cation of this resolution would terminate the precautionary suspension.

Sea Spain Marti

Director of the AEPD

938-131120

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es