File No.: PS/00022/2021

RESOLUTION OF PUNISHMENT PROCEDURE

Of the procedure instructed by the Spanish Agency for Data Protection (as regards hereafter, AEPD) and based on the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the claimant party one) dated August 6, 2019 files a claim with the AEPD. The claim is directed -among others- against ORANGE ESPAGNE, S.A.U. with NIF A82009812 (hereinafter, ORANGE) by the following reasons:

“I want to report the processing of my data by Orange and Banco Santander, which has allowed fraud to be carried out on my accounts bank accounts of almost 15,000 euros.

Regarding Orange, someone impersonated my identity in front of an operator and consi-
He guided me to change my contact email, without the call being made from my mobile. Y later, they got a duplicate of my SIM card, an essential step to get the access data to my online banking.

Upon noticing, despite having put a safeword for any procedure with Orange operators, they have not always asked me (especially the first few days), so I can't be sure I can happen again

Regarding Banco Santander, through several calls to the telephone line and access to my keys online with the duplicate of the SIM card, they managed to change change my electronic signature and carry out two cards in my name and several operations (transfer of credit from said cards and transfers from my accounts to other strangers), all this in a short period of time (from July 22 to 23

July, it is believed that from 7:30 p.m. to 1:00 p.m. that I realize), without

the Bank to contact me upon detecting so many movements (on

7 moves on 3 counts).

Apart from the claims filed against both the Bank and Orange, and

the judicial measures that it can carry out, I would like this Agency to take

precise and timely measures. (…)"

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

(Pontevedra), dated July 24, 2019, with certificate number ***CERTIFICATE.1

in which it states:

'That the denouncer today, around 09:00 a.m. verified that her telephone

XIAOMI Mi A1 mobile phone-with number ***PHONE.1 of the company ORAN-

GE, with IMEI's number ***IMEI.1 and ***IMEI.2, stopped working.

He went to the ORANGE store to ask what had happened, checked

store than the SIM card ***SIM.1 that was installed in the phone

mobile phone did not work, so they made a new SIM card ***SIM.2.

The store employee realized that the SIM card she had installed in her

phone did not match the one in the ORANGE database.

That the SIM card that appeared in the ORANGE database is ***SIM.3.

That at the time that the deponent installed the new SIM card ***SIM.2 she received

two text messages (SMS) from SANTEVIÓS, with an SMS code to transfer

5,000 euros and an SMS from INFOSNET with an SMS code to transfer

reference of 5000 euros.

That the demonstrator, once the change request form is delivered

notice that the email ***EMAIL ACCOUNT.1 does not correspond

with the email provided to ORANGE. That the email you provided is ***ACCOUNT

MAIL.2(…)

That the protester gets in touch with ORANGE by phone through the

1470 and they inform ORANGE that two calls were made, one to change

change the email and another to request the duplicate of the SIM card, call

calls that were made on 07/22/20219, one at 2:00 p.m. and the other at

19:15 hours stating the number of the latter ***NUMBER.1.

That from the ORANGE store they enter the user profile and it is observed that

there are five calls to the telephone number ***TELÉFONO.2 that corresponds

to Santander's online banking (...)

That the protester examines the movements of her three bank accounts and

of his two cards and observe:

Which unknown author(s) had made a transfer of the VISA card

***VISA.1 for the amounts of 700 and 500 euros to ***ACCOUNT.1 (Banco Po-

pular) being the mirror account of the account ***ACCOUNT.2 (B. Santander).

The protester realizes that on July 22, 2019 unknown authors ten

A new VISA credit card with ***VISA.2 numbering was registered.

What unknown author(s) carry out a transfer of the card ***VISA.2 of 5000

euros to the bank account numbered ***ACCOUNT.3 (Banco Popular) being the

mirror account of account ***ACCOUNT.4 (B. Santander).

Which unknown author(s) made three transfers from his bank account

***ACCOUNT.5, (...) were 1000 euros each, sent to the accounts

***ACCOUNT.6 (EVO BANK); ***ACCOUNT.7 (EVO BANK) and ***ACCOUNT.8

(OPEN BANK) that for each of these transfers they charge the amount

of 6 euros.

Which unknown author(s) make a transfer from the account

***ACCOUNT.3(...) to account ***ACCOUNT.8 (OPEN BANK) for the amount of

250 euros, including a charge of 6 euros for expenses.

What unknown author/s of the account numbered ***ACCOUNT.1 (...) rea-

Three transfers were made, the first being for the amount of 5,000 euros to the

account ***ACCOUNT.6 (EVO BANK). A second transfer of 250 euros to

account ***CUENTA.8 (OPEN BANK), a third transfer of 250 euros to

the account ***ACCOUNT.8 (OPEN BANK). (…)

Likewise, it provides proof of receipt of "Request for changes in the service

Postpaid mobile communications” dated July 23, 2019, which includes the

email of the impersonating person and the new assigned SIM card number.

It also provides the list of calls from said SIM to the telephone line of the San-

tander (***TELÉFONO.2), and a summary of the transfers and deposits made without

Your consent.

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 September 30, 2019, the claim was transferred to

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

In response to said request, ORANGE stated -among other arguments- that

Next:

“(…) The aforementioned facts had already been made known to Oran-

ge by the claimant, this company proceeding to the analysis of the facts

rights and the achievement of a solution in favor of the claimant prior to

ity to the notification of the request for information that concerns us, giving

satisfaction as well to your claim.

Well, after carrying out the appropriate analysis and checks on the

In this case, it was verified that after the acquisition of a SIM card (...) that usually

It has a high influx of public to speed up certain procedures, such as the

payment of unpaid bills, recharges of prepaid cards, etc.), is provided

yielded (...) on July 22, 2019 at 6:52 p.m.

It is interesting to note that (...) it was carried out (...) in breach of the guidelines established

given by this mercantile (...).

(...).

Second. - Report on the measures adopted to prevent the occurrence of

Similar incidents, implementation dates and controls carried out to confirm

test its effectiveness.

In the present case, as soon as Orange has been aware (...), he has

reinforced and strengthened the Protocols implemented for the processing of certain

undermined acts (among which are the duplication of SIM cards) is-

establishing greater controls and identity verification systems for this purpose.

with the aim of ensuring that this situation does not happen again.

Indeed, it comes to show that, in the first place, Orange has eliminated the

possibility of (...), thus limiting the operations permitted in the aforementioned (...)

from July 29, 2019.

Secondly, and as an additional measure, Orange has adopted the decision,

with implementation date September 20, 2019, that, (...) (among which

is found, (...), due to the associated risks inherent to it), cannot be

processed through (...), but the user is obliged to activate it (...)

(after successful authentication).

This new management model has been implemented in order to prevent

situations similar to the one at hand are repeated. We accompany as docu-

Attachment No. 1 to the aforementioned new model.

In this sense, for a better understanding by the Agency to which we have

We have the honor of addressing you, it is convenient to provide greater detail in the explanation

of this new request management model and activation of duplicates of

SIM cards.

In order to achieve greater expository clarity, it is important to differentiate two modes:

differentiated procedures or actions in requests for duplicate cards

SIM:

a) (…). The request must be made:

- (...).

- (...).

b) (...) must be carried out:

- (...).

- (...).

(...).

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

February 2020, in the file with no. of reference E/08994/2019.

SECOND: On November 27, 2019, the director of the AEPD, before the no-

news that appeared in the media regarding the use of practices

fraudulent based on the generation of duplicate SIM cards without the consent

protection of their legitimate owners in order to access confidential information with

criminal purposes (known as "SIM Swapping"), urges the General Subdirectorate of

Data Inspection (hereinafter, SGID) to initiate ex officio the Preliminary Actions

Research aimed at analyzing these practices and the existing security measures.

try to prevent it.

Namely:

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

| Economy | THE COUNTRY (elpais.com)

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

5/99

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

THIRD: B.B.B. (hereinafter, the claimant party two), on March 12,

2020, files a claim with the Registry of the Murcia City Council, which is

registered with the AEPD on June 5, 2020, directed against ORANGE, by the

following reasons:

“On January 8, 2020 they made me a duplicate of the SIM card without my code.

knowledge or consent. They took over my phone line. They asked cla-

go to Bankia and they refunded me 300 euros from Barcelona, Plaza de

Catalonia 1, Sant Boi de Llobregat. They have made me identity theft.”

Along with the claim, provide a complaint with the report number XXX/YY dated

January 9, 2020, presented before the General Directorate of the National Police in the

dependencies of San Andrés (Murcia), in which it states:

“That on the day of the date the complainant's wife receives an SMS which informs her

way that through the number of the decedent has requested a duplicate card-

ta of your phone number.

That the declarant states that he has not authorized such an operation with his number by

so he contacts his phone company, ORANGE, to confirm-

dole this the processing of the duplicate, alleging that it may have been a mistake

by ORANGE.

That the declarant at that time realizes that he does not have coverage in

your mobile phone.

Who decides to check their bank accounts realizing that they have suspended

brought 300 euros from an ATM located at the scene without authorization

tion. (…)”

Likewise, it also provides the response letter from ORANGE dated January 20,

2020, in which they confirm the correct activation of the voice service, a compensation

compensation for the inconvenience caused equivalent to a full month of the con-

treated, and apologize for the inconvenience caused.

On June 26, 2020, the claim was transferred to ORANGE, so that

proceed to its analysis and respond within a month.

In response to said request, ORANGE stated -among other arguments- that

Next:

“In the first place, it should be noted that the duplicate SIM card exposed in the

requirement that concerns us, was detected by Orange the same day of its activity.

vation, 01/08/2020, by associating the activation of the line (...) to the IMEI (...).

In relation to the foregoing, the aforementioned facts had already been brought to light.

acknowledgment of Orange by the claimant, this company proceeding to

analysis of the facts and the achievement of a solution in favor of the claim

prior to the notification of the request for information that

concerns us, thus giving satisfaction to your claim. In this sense, Orange

proceeded to respond to the notified Official Claim, (...).

In this sense, after performing the appropriate analysis and verification of the

case, it was verified that the activation of the duplicate SIM card of the line ***TE-

LÉFONO.3, was made on 01/08/2020 (...). The duplicate card (...).

In that sense, after an exhaustive study of the circumstances of the case that

concerns us, Orange proceeded to (...).

For all of the above, this company is unaware of the reasons that have led to re-

claim before the Agency to which we have the honor to address the facts that

bring cause of the present requirement, being the same refined and informed

two to the affected months ago.

Second. - Report on the measures adopted to prevent the occurrence of

similar incidents, implementation dates and controls carried out to verify

test its effectiveness.

In the present case, as soon as Orange was aware (...), he

has reinforced and strengthened the Protocols implemented for the processing of

completed acts (among which are those of duplication of SIM cards)

establishing greater controls and identity verification systems for this purpose.

with the aim of ensuring that this situation does not happen again.

In this sense, for a better understanding by the Agency to which we have

We have the honor of addressing you, it is convenient to provide greater detail in the explanation

of the technologies used by my represented in the processes of identification

tion of the identity of the owner. (…)

On said claim fell resolution of ADMISSION TO PROCESS dated 31

August 2020, in the file with no. of reference E/05031/2020.

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, three requirements were made:

information sessions addressed to ORANGE, on different dates:

Secure Verification Code Requirement

First

***CODE.1

C/ Jorge Juan, 6

28001 – Madrid

Required date

I lie

01/13/2020

Notification date-

tion required

I lie

01/13/2020

www.aepd.es

sedeagpd.gob.es

7/99

06/23/2020

06/25/2020

Second

***CODE.2

***CODE.3

Third

09/17/2020

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

following information:

09/16/2020

1. Information on the channels available to customers to request a duplicate SIM card crash. (Telephone, Internet, shops, etc.).

2. For each of the routes available, detailed information is requested of the procedure established for the attention of the requests, including the controls for the verification of the identity of the applicant including the data and documents required from the applicant, as well as the details of the verifications tions that are made on them. In case of shipment of SIM card by co-mail, detail of the controls and requirements established on the direction of delivery he saw.

3. Instructions given in this regard to the staff that attends the requests for their attention. Documentation proving its dissemination among the companies employees dedicated to said tasks, internal or external to the entity.

4. Information on whether the performance of the controls to verify the identity is reflected, for each request attended, in the Information System mation of the entity. Documentation that accredits it in your case, such as screen pressure of the buttons (check-box) or other documentation according to the method used.

5. Reasons why it has been possible in some cases to supplant the identity of clients for the issuance of SIM duplicates. Reasons why The implemented security measures and controls have not had an effect.

6. Actions taken by the entity when one of these cases is detected. Information on the existence of a written procedure and a copy of it in affirmative case. Actions taken to prevent cases of this type from occurring produce again, specifically, changes that may have been made on the procedure to improve security.

7. Number of cases of fraudulent duplicate SIM requests detected

two throughout the year 2019.

Total number of mobile telephony clients of the entity.

In the second of the requirements, dated June 23, 2020, the following was requested:

following information:

POINT 1

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

tion of our request dated January 16, 2020, within the framework of

this same file:

A). In the case of the ORANGE brand, it is indicated that (...)

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

are processed (...), including all the assumptions or circumstances alluded to.

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

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

how you should assess the client's circumstances to access the procedure

(...).

B). A copy of the established procedure is requested where the controls are recorded in

the case of processing applications (...) for the ORANGE brand. (In the information

information provided are not described, indicating in the table of controls “Not available

ble”).

A copy of the security policies (SIM request) is requested for the brand

ORANGE, clearly stating the data requested according to the different

recent cases, including all assumptions.

A copy of the specific instructions given to the operators for this is requested

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

C) A copy of the security policies is requested (SIM request and activation)

for the JAZZTEL and AMENA brands where the data that is

requested according to the different cases, including all assumptions.

A copy of the specific instructions given to the operators for this is requested

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

D). Information on the controls established to process the change of address

e-mail address of a user.

Implications of an email address change on activation

of a new duplicate SIM. Way in which the alleged supplanters

have been able to activate a new SIM by previously changing this user data.

E) For all brands, in home deliveries, information is requested on

whether it is possible to change the SIM delivery address and under what circumstances

and controls.

F). In the table of controls provided it is mentioned, in the cases of companies of

messaging: "Delivery without validation of Identity Document".

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 to be carried out by the delivery person.

POINT 2

List of 20 cases of SIM duplicates claimed as impersonation of

identity or fraudulent by customers, of the ORANGE brand. The listing will include

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

those claimed that happened as of January 1, from the first, as a result

crops

up to 20.

It is requested to indicate in the list only:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

9/99

- 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) Circumstances for which it was processed (...). Information if it was verified (...).

It is requested to provide documentary accreditation.

B) Reason why SIM duplication was possible in this case. Accreditation

of the controls that were passed on the identity of the applicant both in the pro-

pia request (...) as in the activation of the SIM.

C) In this case, the email address was changed prior to the

request.

Information is requested on how they changed the customer's email address and credit

Documentary edition of the controls that were passed for the identification of the

client.

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

documentation of the following aspects:

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

future phishing attempts.

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

with the point of sale.

- Whether changes have been made to the procedure to prevent future cases

Similar.

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

resolution of your case.

In the third and last of the requirements, dated September 16, 2020,

requested the following information:

POINT 1

On the list of 20 cases of SIM duplicates denounced/claimed faci-

listed in the previous answer: (whose content is considered to be fully reproduced)

duced in this act of proceeding):

A. In the cases of request and delivery at the point of sale, a copy of the

DNIs or identification documents provided by the applicants for the change of

SIM.

B. In the case of application (...):

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

security policy. If the authentication was performed through (...), provide do-

supporting documentation.

- Detail of the circumstances that concurred to access the transfer.

mitigating the telephone request.

C. For each of the application cases (...):

- Information on whether prior (less than 2 days) to the request of the

SIM has proceeded to the change/request of app access password for

the customer's account. Provide supporting documentation.

- Information on whether in the cases of application or prior modification of the

password, the system security procedure “(…)” has been followed.

Provide supporting documentation.

If the password has been changed by other means, inform which have

been and provide supporting documentation.

D. SIM Activation.

For each of the cases of courier delivery:

- Information on the way of activating the card.

- In case of face-to-face activation at the point of sale, a copy of the document is requested.

identification document presented.

In case of telephone activation, recording of the call during which the

applicant exceeds the security policy.

In case of activation by means of (...), it is requested in general if

requests some additional identity accreditation from the client to activate the

card, in addition to the entry credentials to (...).

POINT 2

About the following case presented before this Agency: (whose table is given by in-

fully reproduced in this act of procedure):

A copy of the DNI or identification documentation provided is requested, as well as the rest of the

associated documentation, provided by the applicant.

Detailed information is requested on the type of alert that was generated in the system

and IMEI check, according to statements in the letter addressed to the affected "(...)".

Time elapsed between SIM duplication and line restriction.

Actions undertaken by the entity in each case, including accreditation do-

detail of the following aspects:

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

future phishing attempts.

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

with the point of sale.

- Whether changes have been made to the procedure to avoid future cases

Similar.

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

resolution of your case.

FIFTH: On January 28, July 1 and September 24, 2020, ORANGE is

tenders the extension of the legal term conferred to answer said requirements.

On January 31 and July 15, 2020, the Deputy Director General of Inspection of

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

which must be computed from the day following the day on which the first

term granted.

SIXTH: In response to the three requirements made, ORANGE provided the following

following information that was analyzed by this Agency:

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

Required sections according to numbering order:

1.- Information on the routes available to customers:

- (...).

- (...).

- (...).

2.- Detailed information on the procedure:

The control measures in the request and activation of the duplicate SIM are available

inks depending on the brand and the channel used to request the duplicate of the

SIM:

ORANGE brand:

- (...):

(…)

- (...):

(…)

- (...):

(...).

- (...).

JAZZTEL Brand:

- (..).

- (...).

(…)

- (...):

- (...).

- (...):

- (...).

AMENA brand:

- (...).

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

12/99

- (...).

- (...).

- (...):

(...).

- (...):

- (…)

- (...):

-(…).

- (...):

-(…).

(…)

3.- Information on the instructions issued to the operators:

(…)

4.- Information on carrying out the controls:

(…)

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

number of clients:

(…)

6.- Actions undertaken by the entity:

(...):

-. (...).

-. (...).

-. (...).

-. (...).

-. (...).

-. (...).

-. (...).

General measures implemented in different brands.

-. (...).

-. (...).

-. (...):

-. (...).

7.- Regarding the number of cases of fraudulent requests for SIM duplicates detected

ted throughout the year 2019, the entity has stated:

“(…).”

Regarding the cases presented to the agency:

CLAIMANT ONE:

-. Previous Actions: Email address temporarily changed.

prior to SIM request. Information has been requested on how they changed

the customer's email address and documentary evidence of the controls

that were passed for the identification of the client, indicating the representatives

ORANGE teas(…)

.- Change request: Duplicate provided (..) (already withdrawn).

.- Activation (...).

In the fragment of the call that was recorded, (…). The agent wanted in-

travel through (...). Subsequently, the agent (...) defined in the procedures

you're from ORANGE.

. - Damages: Fraudulent banking operations are reported using

SIM copy.

. - Actions undertaken by the entity, including documentary accreditation

such of the following aspects:

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

likely future phishing attempts.

(...).

< If internal investigations have been carried out to clarify the

chos with the point of sale.

(...).

< If changes have been made to the procedure to prevent fugitive

similar tours.

The actions taken to avoid cases of “SIM card changes

not consented” are:

- As stated above, (...).

- In cases of change of SIM without consent that have been pro-

duced (...), it has been found that the salesperson who attended the

defrauder (...).

As a reactive measure in the face of this lack of diligence, ORANGE applies

in these cases a penalty of XXX € to the point of sale that does not

observe the document validation policy.

- In addition, until September 20, 2019, it was possible to

dad in Orange that (...). As of the indicated date, and before the

Numerous cases of unauthorized SIM changes made through

see (...), this possibility is eliminated in the Orange brand, with the only

except for the period from March 16 to June 28

due to the extraordinary measures adopted by COVID-

19.

- They have been deleted (...). In this sense, it is intended that the policy

of authentication is increasingly strict and makes it difficult to commit

fraud.

- New customer authentication measures have been implemented

(...) as the one related to (...), which is used as a safe and true data

to pass strict security policy to the client.

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

resolution of your case.

After repeated attempts to contact the affected, finally

was able to locate and was informed of the steps to follow.

(...) We try to answer as many questions and other procedures as possible.

arise to the affected client and the cost that has occurred is paid.

change the SIM card to recover your line after

that unauthorized change.

They provide a screenshot (...) of an interaction with the client

where the contacts maintained with the client are reflected.

CLAIMANT TWO:

-. SIM change request: (...).

They provide a copy of the DNI provided as well as a complaint for theft

of ID. The representatives of the entity have stated that (...).

(...).

It is noted that some documents are missing to be delivered according to the

ORANGE protocol. (...):

- (...).

- (...).

-. Damages: Fraudulent banking operations are reported using the

SIM copy.

-. Controls: (...) ORANGE has a (...), used as a measure of

security in the prevention and detection of fraud. (...). In the specific case

SIM card duplicates, the system works as follows:

- (...).

- (...).

(...).

About the time elapsed between the duplication of the SIM and the restriction of the

line the representatives of ORANGE only state that in the

the same day.

On other cases not filed with the agency:

Provided the list the breakdown of the 20 cases is as follows:

- (...).

- (…)

- (...).

Required (...) for face-to-face requests/collections at the store, the representatives

tes of ORANGE contribute 4 (...) for 4 of the cases. It is verified that two (...). In other

case is provided (...). They indicate that for two of the cases it has not been possible to obtain the

information required by the point of sale but a total of 5 (...) of the 9 are missing

required.

(...):

- (...).

- (...).

Required the recording of the conversation for the telephone case, as well as documentation

accrediting the application (...) where appropriate, the representatives of the entity in-

They say that they provide a copy of the recording of the activation of the corresponding card,

stating that:

“(…).

(...).”

ORANGE has been asked to detail the circumstances that occurred to

to access the processing (...), indicating the representatives of the entity that

Duplicate request was made on 04/22/2019 and during the period

from March 16 to June 28, 2020, due to the exceptional measures adopted

das as a result of Covid-19, we proceeded to enable (...) as a measure

of contingency, to manage the request of change and duplication of SIM card.

Regarding the cases of activation by means of (...), it has been requested in general, if

some (...) is requested from the customer to activate the card, in addition to (...). Given this, the

representatives of the entity have stated:

"(…).

(...)."

SEVENTH: On August 27, 2020, commercial information is obtained on the

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

4,779,670,000 euros. The share capital amounts to 1,097,665,000 euros.

EIGHTH: On January 27, 2021, information is obtained from the National Commission

tion of the Markets and the Competition on the lines of mobile voice telephony by

type of contract and by segment, the results being:

OPERATOR

PREPAID

POSTPAID

ORANGE

Residential

2,569,156

Business

0

Residential

8,953,958

Business

2,204,408

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

sanctioning procedure against ORANGE, in accordance with the provisions of articles

Articles 63 and 64 of Law 39/2015, of October 1, on Administrative Procedure

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

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

article 72.1.a) of the LOPDGDD as very serious, and may be sanctioned with a

administrative fine of 2,000,000.00 euros (two million euros), without prejudice to

whatever results from the instruction.

The Initiation Agreement is notified to ORANGE, on February 15, 2021, through

instead of Citizen Folder, according to confirmation that appears in the file.

TENTH: On February 16, 2021, ORANGE requests the extension of the term

to adduce allegations and provide documents or other evidence.

ELEVEN: On February 17, 2021, the instructor of the procedure agreed

gives the extension of the term requested up to a maximum of five days, in accordance with the

provided in article 32.1 of the LPACAP.

The Extension Agreement is notified to ORANGE on February 18, 2021.

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

TWELFTH

form, a letter from the representative of ORANGE in which he adduces allegations and after

party what is appropriate to his right, ends by requesting the file of the procedure and subsidiarily, that the AEPD consider the fundamental mitigating circumstances das and finish the procedure by means of a warning and with the imposition of the obligations to implement suitable corrective measures.

In summary, he argues that:

PREVIOUS.- EXISTENCE OF A WORKING GROUP ON DUPLICATION OF SIM CARDS LEADED BY THE AEPD.

The fact that within said Working Group (GT) it is required to ORANGE to share all the information regarding the processes and multiple ple preventive and reactive controls for the prevention and management of this type of fraud, should lead us to think that such sharing is done within of the most absolute and strict framework of trust and full confidentiality.

Public-private partnerships provide the Administration with the advantage of that, companies specialized in certain services, contribute the knowledge and the best solutions on issues that are of interest to consumers. midores and for citizens.

Also noteworthy are the work tables opened with the Ministry of Inside. During 2020, the collaboration with the Security Forces and Bodies State Security (FCSE), has meant more than 40,308 requests attended and derived from the Courts; 45,552 requests attended and derived from the Judicial Police and 50,056 telephone taps carried out (among discharges, dismissals and dismissals).

In addition, ORANGE staff have been awarded the Cross of Merit Civilian with white badge.

Likewise, he has actively participated in the report of the study paper about the risks derived from the use of the network by minors in the

Senate in the signing of a High Level Protocol.

For its part, the AEPD has considered that this is the ideal time to propose

have millionaire sanctions to the same entities with which it is sitting

to agree on common measures, an unprecedented and surprising precedent.

The appropriate thing would be to wait to have some conclusions and, once known and

given an adequate period to achieve its implementation, it is then, when

requires the operators to certify their compliance and in case of not doing so,

done, that is when sanctions are proposed.

The WG meetings have suffered delays due to the COVID pandemic

19, which have slowed down their periodicity -delay from that scheduled on 03/16/2020 to

4/12/2020- which has harmed the analysis of the problem and the proposals

ta and implementation of improvements.

It seems that the Agency has no pretense of complying

to the principles of institutional loyalty that are presumed in any relationship

of public-private collaboration, meanwhile, at the same time that it requests the collaboration

elaboration, information, active and effective participation in the GT, initiates a procedure

sanctioning procedure that deals with the matter dealt with in the GT.

The AEPD crosses the most elementary limits of institutional loyalty that are

boasts a public body in this collaborative framework.

The opening of this procedure and others like it makes it extremely difficult to

existence of a framework of trust between ORANGE and the AEPD, and the entire

national telecommunications sector.

ORANGE wants to record that this way of proceeding seriously affects

to the principle of trust that he presumed to be able to deposit in the AEPD and su-

poses a risk to the objectives of the WG, which will be subject to internal analysis and

probably sectoral regarding the collaborative framework with Administrative Authorities.

initiatives that pursue this common good of citizens with action plans

tion and joint collaboration.

FIRST. - INCORRECTION AND LACK OF ACCURACY IN THE ASSESSMENTS-

TIONS ON SIM CARD DUPLICATE FRAUD.

The description made by the AEPD contains various statements

inaccurate and technical errors that lead to an inappropriate interpretation

of the facts and their legal consequences.

SIM cards do not serve “to identify the subscriber before the telephone network

mobile”, but rather identify a telephone number, without including any information

tion that allows third parties, other than the telecommunication operator itself,

nes with which you have contracted the service, identify the subscriber.

The fact that the subsequent use of the duplicate SIM is aimed at the co-

mission of other crimes -carrying out fraudulent banking operations-,

under no circumstances can be considered within the scope of responsibility

from ORANGE. By itself, this act is not enough to perform operations.

bank transactions on behalf of the initial holders of the SIM cards, but rather

an additional and independent criminal activity must take place.

The use by banking entities of a double factor system of

authentication that implies the sending by SMS of the ratification keys for the

carrying out certain operations is an operation on which ORAN-

GE does not have any decision-making capacity.

There is no causal link between identity theft for the

issuing a duplicate of the card and carrying out banking operations

fraudulent or other types of identity theft operations in another

type of online platforms, but what is really produced is a usurpation

initial disclosure of the identity of those affected before the bank and derived

of it and subsequently, the confirmation of the operations would take place

by using the keys sent by SMS.

This possibility would only occur when the means established to guarantee the

security corresponds to sending an SMS, since the double factor of

security (known generically as "authentication systems with

One-Time Password" or "One Time Password") does not have to be configured

necessarily be arranged in this way, this being an option whose choice

It is the responsibility of the banking entity and/or the corresponding user, given that many

many platforms can be used as a means to notify the second factor

authentication, SMS, email, or code generation applications

temporary Google Authenticator type or similar.

These facts are perfectly known by the AEPD, which even has

published on its website a publication called "Identification in services of

online payment".

Therefore, the considerations expressed by the AEPD in the Initial Agreement

that the ultimate consequence of identity theft before

ORANGE is the performance of unauthorized banking operations must be

nuanced, since this possibility only exists when this is the chosen medium.

do for the confirmation of the operations and also, previously and necessarily,

the bank identity itself or the user have not taken sufficient diligence

cient for the protection of the initial means of identity verification

(first factor) that allow access to the tool from which the

nan banking operations.

The same effect could also occur without the need for spoofing.

identity. This would be the case in which a subscriber decided to cancel his number.

phone number and later was the subject of portability. If the user

rio did not adopt due diligence to update its information in the face of the differences

different entities to which you have provided your telephone number

as a means of authentication, it would enable the third party that received that number

number could receive the confirmation messages issued by said entities.

des The same effect could occur in the case of theft of a terminal that the user

had not adequately protected (allowing access to its content without

need to use passwords, fingerprints or other security measures).

Therefore, illegally obtaining the duplicate SIM card is not enough

to carry out fraudulent banking operations, nor does it have to con-

occur to allow them to be carried out, so it cannot be attributed

generically this responsibility.

However, ORANGE is not exempt from the problems derived from the potential

use of duplicate cards for illicit purposes. It is for this reason that it has implemented

mented reinforced security mechanisms in relation to the conditions

for your request.

SECOND. - UNFOUNDED GENERALIZATION OF NE- CONSEQUENCES

GATIVES ASSOCIATED WITH THE ISSUANCE OF THE DUPLICATE OF THE CARD

SIM.

Many of the statements contained in the arguments put forward by the

AEPD are inaccurate or erroneous.

It is not true that "by getting a duplicate SIM card, the impersonators

they will automatically have access to the contacts and will be able to access all

applications and services that have as recovery procedure of

send an SMS with a code to be able to change the passwords".

It should be noted that these can be stored "physically" on the cards

SIM, so this information would not be in the duplicates that can be issued.

disposed of, but would remain only in the original SIM, under the control of your

owner, unless the user has chosen to store them in environments associated with

Android or Apple, in which case the operator does not have the capacity to act either.

therefore, once again, the AEPD makes an erroneous statement

whose sole purpose is to justify the hefty penalty proposed based on the

alleged damages that have been caused to the holder of the numbering.

Regarding the possibility of accessing email, bank and

others mentioned, it is obvious that the duplication of the card does not allow, by itself, the

access to them, but it is necessary, at least, to know the identifier

of the user to be able to access any of the accounts.

Furthermore, it should be noted that when the impersonator addresses

ORANGE to request the duplicate already has a lot of relative information

to the interested party, which is necessary for the management of the request. Therefore, the

Obtaining this information, in a presumably illicit manner, is the responsibility

liability of third parties or of the owner of the data, existing in many cases

reckless behavior of the latter in the custody of their information

personal tion.

The responsibility of ORANGE cannot extend beyond those

issues that fall under its scope. Interpret the opposite sig-

means making it responsible for the security of the information guarded by ter-

zeros, and even of the possible negligent actions of these or of the own

owner of the data, as well as the fact that there are real mafias

specialized in committing crimes.

With regard to the possible violation of security principles,

data confidentiality and proactive responsibility, although it is true that

there is an incident related to information security, it has not been

produced in purity an access to personal data of the clients as con-

sequence of this The only information the impersonators would have gotten

followed is the telephone number and, if applicable, the verification codes for

lization of banking operations that, although it is confidential information, under

No concept can be considered as personal data by itself.

mos.

Therefore, although data is processed during the duplicate request process

personal, this does not imply that there is an illicit treatment derived from the lack

due diligence of ORANGE, but rather that ORANGE performs these operations on request.

sending data to who is supposed to be its owner and to make verifications, not

having provided any type of personal information that did not have initials

mind the applicant.

In this regard, it should be noted that the personal data processed in a

illegally are not obtained from ORANGE, but are obtained by impersonators

previously from other sources (the interested party or third parties responsible for

such data). Even, as stated in the file, the crime of impersonation

is accompanied by falsifications of public documents, such as copies of

DNI or alleged complaints filed with the police, which are provided as

means to overcome ORANGE's control measures.

There is no specific regulation that establishes the obligations in relation to

tion with this operation, and the only one that could be considered as a reference,

for having certain similarities in terms of the matter, is Circular 1/2009, of 16

of April 2009, of the Telecommunications Market Commission, which

regulates the initial contracting procedure for telecom services.

communications, and which does not contain any requirement of equitable security

comparable to those that the AEPD intends to require in relation to a procedure

which would be secondary to that regulated in said circular.

Nor has it been proven, nor does it appear in the complaints, any reference

to criminals having managed to obtain personal data from ORAN-

GE, so there can be no question of non-compliance with protection measures

of personal data.

The AEPD, and in very recent procedures, had not been considering that

If there is a breach of security measures in relation to the sub-

positions in which identity theft occurred in exact cases.

identical mind. Thus, we can cite, for example: E-04919, PS-00144-2019,

PS-00235-2020, PS-00348-2020, E-01178-2020.

In none of them is it observed that there is a qualification as an infraction

of the security obligations required in article 32 of the RGPD.

Invokes article 54 of Law 30/1992, of November 26, on the Legal Regime

co of the Public Administrations and the Common Administrative Procedure

(already repealed), in its first section that said: they must be motivated

(...) acts "that deviate from the criteria followed in preceding actions

you". In other words, in the event of the same factual assumptions, the application of solutions

different must be justified "with a brief reference to facts and fundamentals

of law" of the reason for such disparity in order not to violate the principle of

legal security.

The rationale provided is limited to referring to possible vulnerabilities

ties, which in no case are identified, let alone exposed why

they can be qualified as insufficient or inadequate.

It is also noteworthy that it is held responsible for the effects derived from

Other actions that do imply unauthorized access to personal data

those affected, victims of alleged phishing or the like, who do

limit access to personal information protected by other data controllers

treatment.

THIRD. - SUITABILITY AND COMPLIANCE WITH PREVENTIVE MEASURES

YOU ARE IMPLEMENTED BY ORANGE.

ORANGE has carried out a detailed study of its treatment activities

of personal data carried out and has adopted the pertinent measures

so that they are carried out in accordance with the provisions of the RGPD.

Regarding the safety of the process, it has provided evidence of the existence

ence of specific protocols appropriate to the risks identified.

It has organizational measures that have been communicated to all personnel.

party involved in the processing of personal data.

It is important to indicate that the organizational security measures are supported

ted by (...) which is responsible for implementing and operating security, measuring (...).

In order to provide reliability to third parties about the proper func-

By implementing these measures, both technical and organizational, ORANGE maintains

has and certifies Information Security Management Systems based on

in ISO27001 and National Security Scheme.

The existing protocols have been communicated to all those involved in the

management of duplicate requests, including penalties in the

in the event that breaches of the established procedures are detected.

The operations defined have taken into account the risks associated with carrying out

of this type of management and the parameters for its execution have been set

in the knowledge of the people involved in its processing. The number of

cases is negligible compared to the total number of operations carried out.

Although the means and controls have been increasing to guarantee strict

compliance with the established protocol, it is not possible to eradicate the possibility

of its contravention by users, since, ultimately, it depends

fair action by the person processing the application, which is

aware of the instructions to be followed in each case.

The intended solution proposed by the AEPD consisting of automation

total controls to prevent unauthorized actions, albeit hypothetical-

mind could allow a better control of the procedures, it would have a cost

exorbitant since it would imply a systematic monitoring of all the activity

user's identity (by way of example, the system should allow: knowing and analyzing

lyse the content of the conversation held with customers, know and verify

verify the content of all possible documents that may be made available

disposition during the request, validating its adequacy in each case, knowing

see if the answer to the questions corresponds to the existing information,

etc.).

In this sense, the AEPD does not justify in any way the proportionality of the

proposed measure, nor that it was the ideal one taking into account the

of the technique, the costs of application, and the nature, scope, context

to and the purposes of the treatment.

The measure also means ignoring the reality of the actions of users

responsible for carrying out these procedures that fulfill in practice all

quality of the cases with the indications received from ORANGE.

Similarly, it does not take into account the small number of assumptions in the

that a contingency has occurred associated with the request for a duplicate

card, which specifically represents (...) % of cases.

QUARTER. - ORANGE'S DILIGENT PERFORMANCE.

ORANGE has not implemented "static security measures", but has

proceeded systematically to implement improvements in the measures adopted

as soon as it has become aware of the existence of any vulnerability.

In the case analyzed, the personal data of the victims are usurped with

before the criminals go to ORANGE and that precisely

as a consequence of having access to personal information that should only be

being in the possession of the interested party, allow the impersonation of identities to materialize.

ity against ORANGE.

This circumstance in no way prevents the fact that ORANGE has complied with

its obligations in accordance with the provisions of recital 83 of the RGPD to

referred to by the AEPD.

There can be no talk of negligence in any case, since the circumstances

concrete in which the events occur, in which criminals under the

appearance of victims of a robbery and using tricks and fraudulent documentation

dulent with real appearance (...) they manage to deceive the person to whom they are

Request in duplicate. (...). Therefore, it is a sufficient delusion, for re-

dress this "appearance of reality and seriousness enough to deceive people

medium perspicacity and diligence" (thus considered, among many others,

in STS 2362/2020).

Occasionally certain partial breaches of the protocols occur

provided by ORANGE, which in certain cases contribute to the

tion of the end pursued by the fraudsters.

However, this does not allow us to conclude that these facts show "the

a series of vulnerabilities in the security measures implemented and, therefore,

Therefore, the responsibility of ORANGE as responsible for the treatment is inferred.

in terms of negligence, lack of supervision and control”.

On the contrary, the measures implemented by ORANGE are suitable for mi-

to mitigate, for the most part, the risks related to this type of fraud.

In practice, as reported, the efficiency of these measures is close to

100% of the cases.

It must be remembered that, although they could have been punctually breached and

partially by the people in charge of processing some

In addition to verification obligations, there are combined safety factors

two that make it difficult for fraudsters to target. (…)

Only in exceptional cases in which the means used for the determination

develop the scams are especially sophisticated, combined in some su-

position with specific omissions of some of the requirements established by

ORANGE by those involved in the processing of applications, it has been

produced the result of impersonation of the identity of the clients.

In this sense, Circular 1/2016 of the Tax Office can be used as a reference.

General State Office, regarding the criminal Compliance protocols in which

it is argued that “crime does not necessarily invalidate the prevention program.

tion, which may have been properly designed and implemented without reaching

gar to have an absolute efficiency".

According to ORANGE, it has been proven that:

~

It has established adequate protocols for the prevention of impersonations

of identity in the process of requesting duplicate cards.

~

Has duly communicated the content of these protocols and the obligations

nes that correspond to the people involved in the processing.

~

Has made improvements in the processes when it has become aware of vulnerabilities

vulnerabilities, such as reinforcements in the guarantees and limitation of channels

for the request or inclusion of new, more effective control methods (such as

(…) released in October 2020).

~

It has adopted sanctioning measures against breaches of the pro-

tocolos.

~

Has acted as diligently as possible, immediately, efficiently

and executive, in cases in which he has become aware of any fact.

- It has systems for verifying compliance with its obligations

by the people involved.

~

Has filed complaints for the scams committed and collaborates so that they can

It allows the culprits to be identified and similar future assumptions to be avoided.

Consequently, the activity of ORANGE cannot be classified as ne-

negligent, nor has there been a lack of supervision or control.

Invokes STS 1232/2018 of July 18, 2018, which recalls what can

considered as "negligence" or "guilt in vigilando" on the part of a company

sa (company) in relation to the behavior of its employees to collaborate

tors, stating that: "It would be possible, in effect, to contemplate in the abstract a guilt

in vigilance of society, starting from duty -widely analyzed by the

civil doctrine and jurisprudence - that weighs on companies to ensure the

behavior of their dependents, proxies or employees to avoid

that negligent or fraudulent actions of these may cause damage to third parties

who have trusted the company in whose name or on whose behalf they act."

Thus, according to the criterion of the Supreme Court, it would not be possible to hold

to ORANGE even if your employee or collaborator had been negligent in

their actions, since "negligent or malicious actions" would be required on the part

of ORANGE, which under no circumstances have occurred in the cases under

of analysis.

On the other hand, even if it were possible to sanction if the conduct was

qualified as negligent, this same Judgment includes the necessary requirements

cessaries on the content that an accusation of this type must fulfill in a

sanctioning file: "A rating covered by fault in vigilando,

however, it would need one more element to allow affirming the responsibility

in the sanctioning scope (in our case, for tax infractions): a

express, sufficient and detailed justification of the breach of duty

monitoring that the sanctioning body should offer in its resolution, analyze

considering the circumstances of the case and determining what has been the concrete

behavior of the company revealing the infraction of that obligation.

3. In short: a) Conduct such as the one described above cannot be classified as malicious.

concerns us, because -according to the facts that comprise it- it is not possible to speak

of intention or willingness to perform the typical behavior; b) would only fit

affirm in such cases "negligence" if the duties of vigilance are infringed.

lance that weigh on society in relation to the people who act in

his name and provided that such violation appears verified and justified ex-

prey and in detail in the penalty agreement, which must analyze

the circumstances of the case and to what extent the lack of vigilance has contributed

to the commission of the offence."

Similarly, the TSJ of Madrid in its Judgment 568/2020 of 10 Sep. 2020

establishes: "There will have to be, therefore, fraudulent or negligent conduct, whether

gross or slight or simple negligence. And there is no negligence, nor therefore infringement.

tion, "when the necessary diligence has been exercised in complying with the

tax obligations" (article 179.2.d) of the LGT 58/2003)".

In view of the foregoing, the jurisprudence protects the behavior of ORAN-

GE, having established an action protocol prepared taking into account

account the existing risks, which was made available to all those involved.

and that, if they had been followed by these, they would not have accessed the entre-

ga of the illicit copy of the card.

In addition, with regard to the in vigilando responsibility of the company, it is

unquestionable that can only be blamed when it comes to performance

guilty or intentional actions, not negligent as the act has been identified.

tion of ORANGE by the AEPD itself, despite the fact that it is far from being so.

FIFTH. – LACK OF PROPORTIONALITY OF THE PROPOSED PENALTY.

There has been no breach of data protection regulations,

since ORANGE has taken all the necessary technical and organizational measures

sarias to avoid fraud in the request for duplicate SIM cards.

Regarding the duration of the infraction, these are not situations that are

petua in time, but are independent events.

As for the number of interested parties affected, it is not possible to consider the number

of total assumptions as a cause of aggravation without having determined the

concurrence of guilt of ORANGE in each of them.

Regarding the level of damages and losses suffered, it is not feasible to try to

make ORANGE responsible for situations related to the use of duplicates.

two of the card that derive from information security incidents with

which ORANGE has no relation. The duplication of the card does not lead

goes directly, nor necessarily, in fraudulent banking operations, since

that the security measures and the accesses to which they have to carry out the

Banking operations are totally unrelated to SIM card duplication.

Neither can intentionality or negligence be interpreted in their actions. In

In any case, it must be considered diligent and act as a mitigating factor.

tea.

Regarding the degree of responsibility: far from this criterion being an aggravating circumstance,

should be interpreted in your favor. Initiatives such as the use of technology stand out.

girls like (...).

Categories of personal data affected by the breach: SIM card not

allows identity theft, but only serves to receive

tion of the confirmation keys of banking operations in certain

assumptions. But this does not mean that the impersonator can operate on behalf

of the affected, unless the security measures of other

entities, such as the bank.

In this sense and taking into account the concurrent circumstances and the null

guilt of ORANGE, in the event that it is considered that there is some type of

of infringement of the RGPD, the proposal for an economic sanction should be

protected by the adoption of the corrective measures contemplated in the aforementioned

article 58 RGPD, consisting of the warning or warning to the responsible

ble of the treatment and the imposition of the obligation to adopt measures

to carry out the treatments “in a certain way and within a

specified".

THIRD

: Dated April 27, 2021, this Agency received a written

TENTH

of the representative of ORANGE by which he formulates additional arguments to the

previous.

Attach the following documentation:

OF A GENERAL NATURE:

- Document 1: (...).

- Document 2: (...) to follow in SimSwap cases.

- Document 3: Statement issued by SimSwap Risk Fraud.

- Document 4: Content published (...) about SimSwap.

OF A TECHNICAL CHARACTER

- Document 5: (...).

- Document 6: (…).

These allegations and the previous ones have already been answered in the Proposed Resolution.

tion and are reiterated, in part, in the Foundations of Law (hereinafter, FD) of this

Resolution.

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

initiation and presented arguments, dated April 30, 2021, by the instructor

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

terms:

“The claims filed are considered reproduced for evidentiary purposes.

by A.A.A. and B.B.B., its documentation, the documents obtained and generated

two by the Inspection Services before ORANGE ESPAGNE, S.A.U, and the In-

form of previous inspection actions that are part of the file

E/11418/2019.

2. Likewise, the allegations to the

initiation agreement PS/00022/2021 presented by ORANGE ESPAGNE,

S.A.U, on March 8, 2021, through the General Registry of this

Agency, and the documentation that accompanies them:

 Document 1 (minute)

 Document 2 (complaints)

3. Also, they are considered reproduced for evidentiary purposes, the allegations

“complementary” to the initiation agreement PS/00022/2021 presented by

ORANGE ESPAGNE, S.A.U, on April 27, 2021, through the Registry

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

 Document 1: (...).

 Document 2: (...) to follow in SimSwap cases.

 Document 3: Statement issued by SimSwap Risk Fraud.

 Document 4: Content published (...) about SimSwap.

 Document 5: (...).

 Document 6: (...). (…)”

FIFTEENTH: On September 30, 2021, the instructor of the procedure

ment formula Proposal for a Resolution, in which it proposes that by the director of the

AEPD sanction ORANGE ESPAGNE, S.A.U., with NIF A82009812, for infringement

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

72.1.a) of the LOPDGDD, with an administrative fine of 800,000'00 (eight hundred thousand

euros).

On October 4, 2021, through the Citizen Folder, the Pro-

Resolution setting.

SIXTEENTH: On October 7, 2021, ORANGE requests the extension of the

term to formulate allegations to the Resolution Proposal.

SEVENTEENTH: On October 7, 2021, the Agency grants the extension

tion urged.

EIGHTEENTH: On October 26, 2021, ORANGE, makes allegations

to the Proposal for a Resolution in which the allegations are ratified and reproduced.

tions and legal arguments made to the Initiation Agreement (background DUO-

TENTH and THIRTEENTH) and also adds others:

FIRST: INFRINGEMENT.

It is noteworthy that in the FD the commission by the

ORANGE of an infringement of article 5.1.f) of the RGPD based on the facts

by tested by the Agency. This, before even trying to justify

car the reason This proceeding, even if only for formal effects, is legally

inappropriate and could be considered a certain predisposition of the AEPD to sanction

declare it, regardless of the allegations it may make in its defence, given

Note that no such violation has occurred.

SECOND: PROCESSING OF PERSONAL DATA AND RESPONSIBLE FOR THE TREATMENT

TREATMENT.

A number of qualifications are required in relation to the duplication process

of a SIM card involves the processing of personal data.

The information processed during the duplication process of a SIM card is the information

information identifying the owner of the line, not the technical information contained in said

card, with the exception of the MSISDN, since its content is none other than its own

telephone number (preceded by the national prefix).

These and not others are the data subject to treatment carried out by ORANGE as

responsible.

All this information was already known by criminals before requesting

the duplicate, after having previously obtained them illicitly by means of techniques

social engineering such as "phishing" or "spoofing".

Therefore, the statement that "ORANGE is responsible for the

data processing referred to in the exposed antecedents", since in the same

reference is made to other treatments that are not your responsibility.

There is no evidence that any information that may be

contained in the SIM cards, such as the IMSI, much less information about the list

telephone or calls and messages. Regarding the IMSI, there is no proof

ba or indication that this data has been treated for any purpose.

Nor is the statement made by the AEPD that the SIM card is,

in itself, a personal data. The card may contain personal information, but

It is not data and although this information could be considered as personal data by

make the owner of the line potentially identifiable, the truth is that the possibility of

identification by third parties other than the operator would require information

additional information that is not available, so even if they qualify as data

personal, would be considered pseudonymized data.

THIRD: ALLEGATIONS ADUCTED.

1. PREVIOUS ALLEGATION.- EXISTENCE OF A WG ON DUPLICATION OF

SIM CARDS LEADED BY THE AEPD.

The breach of legitimate expectations is not due to the statements that could

having carried out the Agency validating the performance of ORANGE.

The undermining of this principle is due to the fact that the opening of the sanction

tionator is produced within the framework of a collaboration in which the

a specific GT to deal with a criminal activity (“SIM Swapping”), in

whose bosom integrates both the telecommunications operators and the

bank, as well as other Administrations and Authorities involved, created with

the intention of protecting those affected, and whose purpose is to analyze formally

combines threats and defense mechanisms, with the aim of

clarify possible actions that help mitigate the risks of impersonation

of identity.

In this sense, although the participation of the AEPD in the GT does not imply the validation

of ORANGE's performance, it does show the recognition of the pro-

existing problem and the difficulty posed by its prevention: it is a

widespread and recurring problem, which affects multiple entities and

telecommunications operators whose solution is highly complex and, if

The joint will to put an end to these assumptions has been well shown,

eradicate them, it is a complicated objective, given the capacity of

criminals to update their techniques and deploy means every time

more sophisticated to achieve their goals.

In this context, it does not seem logical to require operators, and specifically

ORANGE, the deployment of a diligence of absolute efficiency.

However, it is within this framework that the AEPD decides to open an

tooth, using as a pretext the existence of certain news in

press when you have first-hand knowledge, by the operators

ras, of the existence and characteristics of these crimes.

Moreover, said information was made known to you in the confidence that

All entities present will use the information in good faith and not to

purposes other than those for which the WG was created.

The Agency uses this knowledge to employ it with the objective of sanctioning

trying to hold them accountable for the crimes of which they are victims, the

who is far from loyal and who obviously breaks the trust in

an Authority that prefers to take the sanctioning route before entities that,

you know conclusively, they are working proactively to improve

of security.

On the other hand, it is obvious that the AEPD is bound by the principle of legality.

but it is not true, as it pretends, that it is this principle that calls it to

sanction. The regulations provide for alternative mechanisms for situations in

which the objective should be to improve the security of the operations of

treatment performed.

The function of the AEPD is, in accordance with Royal Decree 389/2021, of June 1,

by which its Statute is approved, that of "supervising the application of the

legislation in force regarding the protection of personal data in order to protect

protect the rights and freedoms of natural persons". For this purpose, their

powers are not limited to sanctioning activity, but article 58 of the

RGPD has corrective alternatives, such as warning, warning,

treatment or, even, order when appropriate that the treatment operations

to be carried out in a certain way and within a specified period.

In this sense, as the AEPD itself recalls, the sanctions have a financial

dissuasive capacity and it is more than evident that they do not need the spur of a

sanction to protect the data of its clients.

2. FIRST ALLEGATION.- WRONGNESS AND LACK OF ACCURACY IN

APPRECIATIONS ON DUPLICATE FRAUD.

The AEPD introduces a theoretical exposition to try to justify that, as

consequence of the access to the duplicate of the SIM card, there was an access to

personal data contained in the card itself.

First of all, it should be clarified that the SIM does not allow access to the IMEI.

As far as the IMSI is concerned, there is no proof or indication that this data

has been treated by criminals for any purpose, therefore, it has not been

accredited that their confidentiality has been affected.

Additionally, it has not been proven that any other information was accessed.

personal training guarded by ORANGE other than that provided by the pro-

pio delinquents obtained through social engineering techniques such as

"spoofing" and "phishing", therefore, ORANGE has not allowed access by

unauthorized zeros to personal information to which they did not have access

previously and, consequently, there has been no breach of confidentiality-

ity.

The AEPD mixes in its considerations the concept of access to data

as a consequence of the duplication of the SIM card with the realization

zation of banking operations.

Any liability arising from the duplication of cards is restricted

would turn, from the point of view of data protection, to the processing of information

information related to the services it provides (consumption associated with

treatment, access to private area, contracts, etc.) and on which there is no

any evidence that it has occurred.

However, the AEPD tries to hold ORANGE responsible and punish for

the consequences of the operations carried out by the banking entities.

Confuses the obligations of diligence in the processing of personal data

with a supposed obligation to provide security for banking operations

in relation to the identity of the clients of these third parties.

That is to say, it transfers the responsibility in the identification by the entities

bank transfers to telecommunications operators.

Banks are solely responsible for the security of their

operations. This is also confirmed by the European Banking Authority (EBA),

that in his “Opinion on the implementation of authentication methods re-

forced”, in its section on who decides on the means to be used

for said authentication (points 37 and 38), rules that the credentials of

security used to perform secure authentication of users of

the payment services are the responsibility of the entity that manages the services of

account (banks).

That banks usually opt for the confirmation system me-

Sending an SMS is a decision of your sole responsibility.

It is a very widespread method and is not particularly secure. Refer to Digi-

such Identity Guidelines: Authentication and Lifecycle Management, from the “National

Institute of Standards Department”, which rules that SMS should not be

use in two-factor authentication, because of the number of security risks

authority to which it is subject in the delivery of an SMS.

For its part, the European Banking Authority (EBA), in one of its responses

to the questions posed by the sector (Qualification of SMS OTP as an

authentication factor | European Banking Authority (europa.eu)), although

pla the SMS as admissible confirmation factor, remember that the use of

Ordinary SMS is not feasible for the confirmation of banking operations,

for not being safe enough according to the standards of the Directive

PSD2.

Additionally, it points out that this type of information is in the public domain.

and refer to three links.

For this reason, the fact that the modus operandi for carrying out fraud

slow banking operations can be carried out using a SIM SWAP not

can in no way be considered an admission of responsibility for the

safety of these operations.

In fact, the operators' diligence is forcing criminals to

look for alternative methods to obtain the content of the SMS. refer to

news and information disseminated by the National Police through social networks

cials.

It reiterates that the responsibility of the operators cannot cover the operations

bank transactions that criminals may carry out as a result of

that the security measures implemented by banking entities

are inappropriate. Cannot take charge of information security

of third parties for the mere fact that they use telecommunications services.

cations.

He argues that the Agency requires strict liability, in which from

a result, a fault is deduced, without any kind of assessment about it.

on the diligence displayed, an interpretation proscribed by Spanish law.

3. SECOND ALLEGATION.- UNFOUNDED GENERALIZATION OF CONSE-

NEGATIVE ACCOUNTS ASSOCIATED WITH THE ISSUANCE OF THE DUPLICATE.

The AEPD has not provided any facts or grounds to support its inter-

provision.

It admits that for the execution of banking operations the delinquent needs

ta, in addition to the duplication of the SIM, additionally access the information

personal information obtained illegally from the bank or from the user, for

which are not a consequence of obtaining the duplicate.

And in what refers to the criminal modalities that seek “other purposes”.

ties”, the arguments used to justify the presumed responsibility

ORANGE are mere speculations, which refer to potential risks

which have neither materialized nor are they the subject of this proceeding and,

from a technical point of view, they are far from correct.

Pretending that access to a SIM card alone allows certain actions

processes, implies an interested ignorance of the functioning of the mechanisms

security isms associated with most, if not all, of

the services referred to.

The ability to access a user's accounts requires information

add-on not available on SIM card. Claims about the ease of

its obtaining lack any foundation and, what is more important, it is not

None of the risks has materialized nor is it the object of this procedure.

to which the AEPD refers, so its inclusion in this foundation

ment is totally inappropriate.

The AEPD refers to 20 cases of duplicate SIM cards when

only the complaints related to two of the

they. Try to increase this number by referring to situations whose

circumstances do not appear or are the object of this procedure is not pro-

transferor and supposes an inappropriate use of information that was fac-

commissioned by ORANGE within the framework of a request addressed by the AEPD and on

which has not been evidenced any non-compliance related to the treatment

lying of personal data.

In relation to the two claims that are the subject of this procedure-

are due to an inadequate application of the established protocols, which

according to statistics they are adequate and efficient and only absolutely

residual mind have been able to be overcome by criminals in their target

of illegally obtaining a duplicate SIM card.

It must be taken into account that the circumstances in which these

impersonations are not irrelevant.

In the case of claimant two, the request for the duplicate is accompanied

page of documents with the appearance of authenticity intended to deceive the

store clerk, who is also offered a believable account in which

informed that the original documentation had been stolen, along with

your wallet. As it is a copy of the DNI, it is not feasible to process it with the

Mitek verification software, since it analyzes physical characteristics and

that are only present in the original of the document.

In these circumstances, the employee chooses to help the person, allegedly

victim of a robbery, whose circumstances could be aggravated precisely

due to the impossibility of contacting and carrying out the pertinent

tints to avoid greater evils.

Ultimately, the clerk opted, breaching the protocol established by

ORANGE, for not requiring the document accrediting the appointment for renewal

of the DNI or the bank receipt accrediting the collection of the last invoice.

Therefore, although it is true that there is a breach of the protocol (which has

been subject to the corresponding sanction), he is induced by the delinquent

account, which created a situation in which he managed to take advantage of the good

in faith of the dependent, believing him to be the victim of a crime, using a

sophisticated and elaborate preconceived plan for this purpose.

Likewise, in the case of the first complaint, the manager breaches the proto-

security code for data verification, and this enables you to

carry out the card application without following all the established controls.

However, this does not make the measures inappropriate, as they have

Its effectiveness has been demonstrated in practically all cases. In this

sense, that the protocol is susceptible to improvement, is an affirmation that has

to be put into context, since their statistical efficiency indicates that they have been

appropriate in (...) % of cases.

Regarding the improvement of protocol compliance controls, if

Although they are desirable, they cannot obviate the presence of the human factor.

ORANGE has given adequate instructions and information to all those involved.

two but it is not feasible to nullify the possibility that people carry out actions

tions contrary to the indications received.

Faced with these risks, there is only room for training and awareness of those involved and

the requirement of responsibilities in case of non-compliance, as has been

fact ORANGE, unless the AEPD suggests that the hiring of employees

with access to personal data is an unacceptable risk and all of them must

be replaced by automated processes.

4. THIRD ARGUMENT. – SUITABILITY AND COMPLIANCE WITH THE

PREVENTIVE DAYS IMPLEMENTED.

The AEPD questions the protocols that ORANGE uses. However, the

The arguments he uses to make this claim are contradictory.

ORANGE has made a total of approximately (…) SIM changes in

2019 without any incidence in the (...) of the cases.

Therefore, following the criteria of effectiveness pointed out by the AEPD itself and

although the desirable thing is always to achieve the cancellation of the risk, it is not possible to

label them as inappropriate.

A materialization of the risk in a percentage like the one we find

cannot be qualified as a lack of diligence in the deployment of measures.

give security

Impose a sanction because in two isolated cases among more than 800,000

an undesired result has occurred supposes adopting a principle of res-

objective responsibility in the sanctioning scope, vetoed by our Ordinance.

Legal procedure, as has been repeatedly reiterated by the Constitutional Court

tional.

Article 28 of the LRJSP, ties the responsibility to the concurrence of fraud

or fault, no longer includes the last paragraph of article 130 of Law 30/1992, it is de-

cir, the possibility of responding "... even by way of simple non-compliance".

The Constitutional Court, since its Judgment 76/1990, has been warning

on strict liability and, in any case, the requirement that the Administration

nistration, when sanctioning, prove some degree of intentionality. Exi-

ge the concurrence of guilt in the degrees of intent and fault or negligence

serious, mere negligence not being enough.

Therefore, the overcoming of the security measures by a third party cannot

to determine by itself that they are not adequate or sufficient.

Refers to files E/05168/2021, E/00536/2016, E/02237/2020 E/

02723/2020, E/06963/2020, E/00722/2020, E/09882/2020 and arguments

of the Agency, exponents of a duality of criteria that causes an evi-

defenseless, he does not know with certainty what to expect, nor what measures are

implement, when they are considered appropriate on certain occasions.

sions, and, in others, constituting an infraction of a very serious nature.

Likewise, it refers to files E/05272/2018, E/07129/2014, E/

08205/2019, E/5441/2018.

It is not understandable that, despite the volume of data affected by the breaches

mentioned, an adequate level of diligence is appreciated and, however, in the pre-

present procedure, where only two interested parties have been affected

two, the level of diligence shown, through

security, detection and correction measures, taking into account the number

number of SIM duplication processes carried out.

Orange is also the victim of an "attack" led by criminal organizations.

them that relies on digital and social engineering techniques aimed exclusively at

mind to overcome the security measures implemented.

With regard to the considerations of the AEPD on greater security

ity of the enabled channels, any channel is likely to be subject to in-

attempted fraud.

ORANGE has eliminated the possibility of (...) (which has reinforced measures)

security in authentication).

The punctual breach and in absolutely isolated cases by a

manager of the identity verification instructions does not imply at all

that the security protocol depends on the will of the intervening manager.

rather, it implies a breach of its obligations which, as has been

informed, has given rise to the imposition of penalties.

Thus, the measures pointed out by the AEPD regarding "the inclusion of these in the

information system, (...), even with controls on the system screens

of information (...)" do not guarantee any improvement in the control of these activities.

give. Any agent could accept the buttons to continue the process

despite not having carried out the specific security measure.

The total employee monitoring options, in addition to not being pro-

portioned in accordance with data protection regulations, would have a cost

disproportionate, considering that it should be exhaustively controlled

all agents potentially involved in an operation of this type

(especially taking into account that the control should be carried out in time

real), when the statistics show that the related incidences are in-

signs.

On the other hand, it has been proven that all the agents have received the training

necessary information and that the information and management is carried out without any inci-

dence in almost all cases.

Additionally, it is possible to verify compliance with obligations,

since the activity of the users is registered.

All of the above, without prejudice to the fact that, in its process of continuous improvement of the

security, ORANGE continues to analyze possible improvements in all its procedures.

you are

In relation to the information detailed in the "Quick Guide", it has a date of

2017 and is provided for the purpose of verifying the measures implemented in a

prior to the occurrence of the events that are the subject of this proceeding and its

progressive improvement, revision and reinforcement.

Regarding the contractual documentation with the delivery companies, it is necessary to

It should be noted that in the two cases that concern us, no company intervenes.

dam or delivery service provider.

The certificates that ORANGE holds, recognized by the National Scheme

of Security (ENS), have a broad scope, which does not only include the

information systems, but there are a series of controls that apply to

the entire organization, in attention to different aspects, including: protection

of data, network security, use of information systems, training and

awareness and security in the human resources process.

These controls are transversal to the entire organization.

Far from wanting to avoid responsibility, what is requested is, precisely,

that such responsibility is limited to the treatment actually carried out, without ex-

assign the corresponding responsibility to other entities, such as operations

tions and transactions carried out by different banking entities.

Lastly, it should be noted that the nature of the fundamental right of the right

cho to data protection does not eliminate the need to examine due diligence

deployed by ORANGE, nor the consideration of the tiny percentage of incidents

cias that have occurred in the SIM card duplication processes.

5. FOURTH ARGUMENT. – DILIGENT PERFORMANCE BY ORANGE.

The wording is totally confusing and contradictory, so that each paragraph

fo seems to affirm the opposite of what the previous one says, to finally finish

projecting an indeterminate lack of diligence as the ultimate reason for the

sanction.

The AEPD considers that it has breached article 5.1.f), the so-called principle

pio of integrity and confidentiality.

He emphasizes the contradictions of the Agency and invokes that it causes him total indepen-

defense, because despite the fact that he has managed to prove in the procedure

compliance with their duty of diligence and being recognized, is subject to

of a sanction proposal for an undetermined reason, before which no

can present any evidence.

All of this leads to the fact that the AEPD is evaluating the responsibility of

Orange considering only one result, constituting an assumption

strict liability, being indifferent to the diligence displayed

in its preventive and palliative measures.

Reasons why they should be discarded:

•

The AEPD recognizes that “The risk approach and the flexible model when

risk imposed by the RGPD […] does not impose in any case the infa-

feasibility of the measures (…)”. However, it intends to penalize

two specific assumptions among almost a million.

•

• Criticizes that in one of the cases (complainant party two) no

has verified the DNI presented despite the fact that "it claims to have

a specific software to verify if the identification documents

are correct (Mitek)”. This is a technical impossibility, not a

error in the security procedure.

It indicates that "ORANGE's behavior is considered to respond to the typ-

title of guilt As a repository of personal data

large scale (...), it must be especially diligent and careful in its

treatment. (...) we are facing a defeatable error, since, with the application

tion of the appropriate technical and organizational measures, these substitutions

identity thefts could have been avoided.” the blame has to

to do with the diligence displayed, not with an objective fact such as the number

mere data processed.

“The infringement occurs not because of the lack of a specific policy of

security for the issuance of SIM duplicates, but because of the need

ity of its revision and reinforcement”. Despite acknowledging that

“ORANGE has acted diligently in minimizing the impact

those potentially affected by implementing new security measures

to avoid the repetition of similar incidents in the future.

The AEPD re-introduces a new criterion for liability

of ORANGE in the cases analyzed, indicating that it "is di-

directly related to the generation of consequences in third

•

•

ros". Transfers to ORANGE the responsibility for treatments on

those who have no ability to control.

• The AEPD continues indicating that it does not share the fact that these

internal protocols or procedures may be considered adequate

squares "as long as they are susceptible to improvement. It is necessary to reinforce the

identification and authentication mechanisms with technical measures and

organizational measures that are especially appropriate to avoid su-

plantations".

This concept of improvement, abstract and generic, would allow us to qualify any

any protocol as inadequate, insofar as any process is susceptible

of improvement.

It includes certain jurisprudence related to guilt, in which

recognizes that it does not concur if it is justified "that the

diligence that was required by the person who alleges its non-existence" or it is indicated

that "there is no negligence, nor therefore infringement, "when

exercised the necessary diligence in fulfilling the obligations.

The liability of a legal person must be assessed on the basis of

of the diligence displayed as an entity, manifested through the

procedures and instructions approved by it.

•

•

However, the AEPD does not state that the risks generated by

third parties (banking entities) and that are their responsibility, would be

mitigatable much more easily if they adopted measures

adequate to improve the safety of the operations they carry out.

Reasons why ORANGE should not be sanctioned:

The confidentiality of the data processed in the duplication process of the

SIM card was previously broken by banks.

ORANGE has no control over this operation nor can it affect its enabling.

tion/procedure/execution.

The succession of suppositions and possibilities cannot serve, under any circumstances,

I accept, as a justification, to impose an infraction on ORANGE without entering

value, motivatedly, the level of diligence displayed and the real facts

mind happened. These threats identified by the AEPD fall outside the

scope of action of ORANGE.

The AEPD considers blame for Orange's conduct, although, far from identifying and

recounting the concrete behavior, is limited to referring to the result. This procedure does not

is in accordance with current legislation, as indicated by the National High Court,

among others, in the Judgment of the Contentious-Administrative Chamber, Sec-

tion 1, of December 23, 2013, Rec. 341/2012:

It should be remembered that the reference to "simple non-compliance" has been removed.

given by the current Law 40/2015, so a lack of diligence would be necessary

qualified.

Invokes the SAN, Contentious Chamber, of February 25, 2010, number of Recur-

so 226/2009".

Mere human error cannot, by itself, give rise to sanctioned consequences.

tioners.

The similarity of this case with the one included in the SAN must be highlighted.

of February 25, 2010: these are intrusions committed illegally,

by organized third parties with high computer knowledge, aimed at

elaborate criminal activity.

The fact that the AEPD and the Courts have been considering

that in the case of technical attacks (hacking), directed against companies,

it is considered that his diligence does not include having the capacity to reject this

type of attacks is interpreted in the opposite way in this case, penalizing

ORANGE because your security measures may depend on the performance

of specific people.

ORANGE, nor its employees or agents, may not be required to

ability to infallibly identify cases of fraud, especially

when it is offered, an "appearance of reality and seriousness sufficient to en-

win over people of average perspicacity and diligence" (so considered, among

many others, in STS 2362/2020).

Provides a copy sealed by the Police Headquarters and communicates the subsequent contribution

supporting documentation (claimant party two), when it is facilitated

litigated by the corresponding Information Units of the Forces and

Security forces.

ORANGE, within the functions included in Law 9/2014, of May 9,

General Telecommunications (hereinafter, LGTEL) and in Law 25/2007,

of October 18, actively participates in the collaboration with the agents

empowered to investigate crimes.

ORANGE should be considered as one more injured party in this type of procedure.

procedures, since it is the entity itself that also suffers a loss and sees

“attacked” their systems and assets.

6. FIFTH ARGUMENT. – LACK OF PROPORTIONALITY OF THE SAN-

PROPOSED TION.

Despite the fact that the AEPD has modulated the amount of the sanction imposed,

considers that, having been diligent in his actions, no imposition

of any penalty.

For the hypothetical case that the existence of a supposed in-

compliance is not proportional.

It should be emphasized that no dissuasive action is necessary, as long as the

supposed object of this procedure has been carried out against

every volitional element of ORANGE.

ORANGE has not obtained benefit, but it has been detrimental. By

which, as far as the need for the deterrent effect is concerned, the mere eating

sion of the crime is a detriment to ORANGE.

Additionally, it participates voluntarily in the GT.

QUARTER. - PRINCIPLES RELATED TO TREATMENT.

ORANGE shares with the Agency the relevance of security measures for the sake of

to guarantee the fundamental right to data protection, however, it must

make a series of nuances:

• The damage suffered by both claimants has been recognized: both received

received compensation from ORANGE.

• Particular circumstances of the claims cannot be considered.

seated nor assumptions within the object of this procedure, the

assumptions and possibilities that the AEPD elucidates: access to applications, use

of social networks, etc.

• Nothing can justify the Agency's Resolution Proposal.

• ORANGE has no control over such procedures or any influence on the me-

security measures used by banking entities.

• Although ORANGE, as data controller, has the obligation to determine

undermine its security measures, it is the person in charge of the treatment who will assume

responsibility, configuring himself as responsible, when he does not follow the instructions

instructions of the former and fails to comply with the purposes and means of the treatment in question,

as stipulated in article 28.10 of the RGPD.

• Reiterate that on two occasions it has been possible to supplant the identity of the

plaintiffs in two SIM card duplication procedures out of a total of

approximately (…) duplication procedures, through sufficient deception,

cannot automatically determine the commission of infringement and absence of

diligence on the part of ORANGE.

• ORANGE does not “provide duplicate SIM cards to third parties”. When

the third one got the duplicate SIM card was because he cheated the agent.

• We are not in the presence of a particularly relevant personal data. The

codes it contains need to be associated with other personal data, in order to

provide identification of the owner. Likewise, there is no evidence of access by supplant-

identity providers to personal data other than those they already knew from

prior to fraudulently obtaining the duplicate SIM card.

• In relation to STC 292/200, the definition and consideration of

of the right to data protection as a fundamental right. What is not

acceptable is the intention of the Agency to impute said infraction, despite having

carried out an appropriate and adequate deployment of security measures,

in the terms of article 32 of the RGPD.

FIFTH. - SAFETY OF TREATMENT.

The legal classification made by the Agency of the infraction imputed to

ORANGE does not include the violation of article 32 of the RGPD.

SIXTH. - GENERAL CONDITIONS FOR THE IMPOSITION OF THE ADMI-

NISTRATIVE.

The treatment carried out does not violate the data protection regulations, since

that ORANGE has displayed an appropriate level of diligence in imposing

tion of the necessary technical and organizational measures to avoid the commission

of fraud in requests for duplicate SIM cards.

The proposed sanction is in any case disproportionate, taking into account the circumstances

Cunstances and content of the alleged infractions.

Recitals 11 and 13 of the RGPD, which refer to guaranteeing the

effective protection of personal data and to do so consistently,

point out that this objective also depends on the fact that “infractions are punished

guen with equivalent sanctions”.

- Aggravating:

1. Nature and seriousness of the infraction:

The loss of control and disposal of personal data does not start when

ORANGE performs the duplication, but it takes place before, at the time when

that individuals gain access to claimants' personal data.

The reference to the role of the mobile phone does nothing but certify the transfer of res-

responsibility towards ORANGE, without taking into account that the limitation of these

risks corresponds to those required by said regulations.

This section does not assess the nature and seriousness of the offense charged.

but the subsequent activity carried out by the indi-

viduos who supplant the identity.

Categorize the nature and seriousness of the treatment carried out by ORANGE,

It requires evaluating the security measures established in the security procedures.

SIM card duplication.

Reiterate that third parties have not had access in either of the two cases.

to the mobile phones of the claimants, and, consequently, neither

to the information that they could store, which is different, in any

case, of the information that a SIM card can store.

2. Duration of the offense:

These proceedings concern the claims of two claimants.

In the case of claimant one, the events have taken place since the afternoon

from July 22, 2019, until the morning of July 24.

In the case of complaining party two, the duration is just a few hours in

on January 8, 2020, since the duplicate was fraudulently made

until the claimant is aware and ORANGE manages the impersonation of

identity.

The time during which claimants do not have access to their SIM card is

less than 48 hours in one case and less than 8 hours in the other.

Therefore, the Agency cannot consider the duration of the alleged infractions.

an aggravating element, insofar as they have been punctual, localized,

ized, identified and managed in minimum periods of time.

The reference to the (...) cases that, together with ORANGE

VIRTUAL ESPAÑA, S.A.U (SIMYO), were accounted for during 2019. No

the relationship of none of the other cases with the infringement has been justified

imputed, nor would this serve to consider the temporal scope of the same.

3. Number of stakeholders affected:

This procedure is limited to two cases.

The existence of more cases of

Duplicate processes of SIM cards with incidents, in both the facts and

Specific assumptions have not been brought up in this proceeding:

No claims have been made by the owners of the data, nor have they been analyzed.

lysed the facts nor the responsibilities derived from them.

Therefore, this part considers that, far from being considered an aggravating circumstance, the infi-

The number of stakeholders should be evaluated as a mitigating element.

4. Level of damages suffered:

ORANGE is not responsible for the identification and verification policies of

customers established by banking entities.

Nor could the banking operations have taken place if the entity

financial institution used another security system in the verification, for example, the

use of biometric data or the identification of the mobile terminal from which

access the bank application, as is already done by some entities.

financial des.

The Agency does not assess the level of damages, as long as it is

limit to indicate that these "multiply" when the duplicate of the

SIM card to a person other than the owner, without explaining the relationship between

this affirmation and the facts object of analysis in this proceeding.

In relation to the origin that indicates to carry out an impact assessment

this, you cannot claim that, in an impact assessment carried out by

ORANGE regarding the issuance of duplicate SIM cards, the possibilities of

from committing fraud in carrying out banking operations through

applications and electronic banking of third parties.

For all of the above, it cannot be affirmed that the duplication process derives

directly, nor necessarily, fraudulent banking operations, since

that the data spoofers need to perform them span many

more information and operations than SIM card duplication.

5. Intentionality or negligence in the infringement:

The Agency requires Orange to have an absolute obligation of result, as long as

the level of diligence is not being evaluated in attention to the measures and

established procedures, but only attends to the result obtained.

The AEPD thus introduces strict liability rejected by our Tri-

Constitutional Court, as we have already indicated, in the jurisprudence that emanates

of the STC 76/1990 of April 26, inasmuch as it cannot be required in the san-

Administration officer.

The Agency also contradicts the jurisprudence (Judgment of the Supreme Court of 23

January 1998): if there is no intentionality or volitional element of ORANGE,

as it is being recognized, and having deployed these security measures

before and after the cases that concern us, as well as procedures

improvement cough; no level of negligence can be imputed to it, as long as

said qualification requires that the legal entity show a minimum degree of

intent, manifested through lack of diligence.

That is why it cannot be considered negligent, as long as

have established appropriate procedures, which have been reviewed and

progressively reinforced.

6. Degree of responsibility of the person in charge:

In the two cases that concern us, the agents failed to comply with the policy of

security and the concrete measures that it imposed.

In addition, it has preventive, technical and organizational measures,

palliative and coercive measures, by which those who do not

comply with the imposed obligations.

Thus, one can only interpret that, far from this criterion being an aggravating circumstance,

should be interpreted in favor of ORANGE.

7. Categories of personal data affected by the infringement:

It has only been possible to determine the processing of identifying personal data

basic, whose knowledge by criminals was prior to the duplication of

the card.

As we have had the opportunity to explain, the theory that the SIM card is

a personal data has no support, but a container of data and codes

gos that only allow user identification if information is available

additional.

Sending SMS has nothing to do with the type of data processed by analysis.

ted at this point.

Therefore, the type of data being processed must be considered as

a mitigation.

- Attenuating factors:

1. Measures taken by the person responsible to alleviate the damages suffered

two for those interested:

The Motion for a Resolution includes preventive measures as mitigating

and coercive, but makes no mention of palliative and compensatory measures.

tions that it has implemented in the two cases that concern us, and that

should be considered mitigating.

2. The profits obtained as a result of the commission of the infraction.

Despite the fact that in the Start Agreement the Agency values the lack of benefit of

ORANGE, we must insist that not only does the absence of benefits

but it has caused damage, it has had to carry out investigations

internal complaints, make compensation to the complainants and reevaluate procedures

ments and protocols.

ORANGE also suffers identity theft by third parties

unauthorized, as they deceive the agents and generate damage to their

service.

To conclude, it considers that the provisions of

Article 76.3 of the LOPDGDD regarding sanctions and corrective measures:

“It will be possible, complementary or alternatively, the adoption, when appropriate,

da, of the remaining corrective measures referred to in article 83.2 of the

Regulation (EU) 2016/679” which indicates that administrative fines are imposed

will put “as an additional or substitute for the measures contemplated in art.

Article 58, section 2, letters a) to h)”.

Taking into account the concurrent circumstances and the null intentionality or

fault of ORANGE, in the event that it is considered that there is some type of in-

fraction of the RGPD, the economic sanction proposal should be replaced

for the adoption of the corrective measures contemplated in the aforementioned article

58, consisting of the warning or warning to the data controller

and the imposition of the obligation to adopt measures to carry out

treatments “in a certain way and within a specified period”

do".

In this regard, ORANGE understands that the initially estimated fine

can be perfectly replaced by the obligatory adoption of measures

rectors.

CONCLUSIONS

1º.- Although the information stored on the SIM card could be considered -

never the card itself - as personal data, it has not been proven that the

themselves have been the object of treatment during the time in which the offenders

many had duplicate SIM cards operational.

2º.- The criminals did not obtain any additional personal data from ORANGE.

nal to those who already had prior to going to ORANGE, obtained from

banking entities and that are used to supplant the identity of the

affected, so that the treatment carried out does not imply an infringement of the

confidentiality of personal data.

3º.- The responsibility of teleoperators for cases of impersonation of

identity in the request for copies of SIM cards cannot cover the operations

bank operations can be carried out as a result of the measures

security of banking entities are inadequate. can't be done

charge of the security of the information of third parties by the mere fact

cho that they use telecommunications services.

4º.- It has been proven that the two assumptions are due to an inadequate

application of the protocols established by ORANGE that, as evidenced by

statistics, are adequate and efficient and only absolutely

residual have been able to be overcome by criminals.

5º.- The overcoming of the security measures by a third party cannot determine

automatically determine that they are inadequate since it implies applying

establish a principle of strict liability in the sanctioning field, vetoed

by our legal system.

6º.- The AEPD has declared certain facts accredited (which has a

security policy in which the mode of action for the expedition is established

of the duplicates; that an infringement of article 32 cannot be inferred, nor

little of article 5.2 and 25 of the RGPD; that there are protocols to prevent

identity theft; that have been transferred to those involved in the

imitation; that improvements have been made after discovering certain vulnerabilities;

that there are penalties for its non-compliance or that it has acted diligently-

when it comes to minimizing the impact by implementing new security measures.

ity).

For all of the above, it is not appropriate to declare the existence of an infringement of art.

Article 5.1.f) of the RGPD nor, consequently, the imposition of any sanction, in

both an adequate level of diligence has been accredited and it has not been accredited

no breach of the duty of confidentiality.

(Underlining, italics, and bold are ORANGE.)

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 are accredited:

PROVEN FACTS

FIRST: ORANGE is responsible for the data processing referred to in the

this Resolution, since according to the definition of article 4.7 of the RGPD

is who determines the purpose and means of the treatments carried out with the purposes

des indicated in its Privacy Policy, among others: the provision of services

of telecommunications, the maintenance and management of the relationship in order to give

compliance with the provisions of the contract signed between the parties (Manage the registration

inside the User and allow access to the activities and tools available through

see the website www.orage.es; carry out the User registration, as well as the maintenance

maintenance and management of the contractual relationship with ORANGE; manage, process and give

response to requests, requests, incidents or queries from the User, when the User

provide your data through the forms provided for this purpose on the Website

www.orange.es, etc.)

SECOND: ORANGE provides its mobile telephony services through three brands

commercials that are: ORANGE, AMENA and JAZZTEL. Each of them has

different operating procedures.

THIRD: On August 6, 2019, this Agency received a claim

mation made by claimant one (file with reference number E/

08994/2019), directed -among others- against ORANGE, after being issued on July 22

of 2019, a duplicate of the SIM card of the line ***TELÉFONO.1, in favor of a

third person other than the owner of the line -the claimant party one-.

These facts were denounced before the Civil Guard of Baiona (Pontevedra), in fe-

cha July 24, 2019, with certificate number ***CERTIFICATE.1 in which the part

Claimant one stated the following:

‘That the denouncer today, around 09:00 a.m. verified that her telephone

XIAOMI Mi A1 mobile phone-with number ***PHONE.1 of the company ORAN-

GE, with IMEI's number ***IMEI.1 and ***IMEI.2, stopped working.

He went to the ORANGE store to ask what had happened, checked

store than the SIM card ***SIM.1 that was installed in the phone

mobile phone did not work, so they made a new SIM card ***SIM.2.

The store employee realized that the SIM card she had installed in her

phone did not match the one in the ORANGE database.

That the SIM card that appeared in the ORANGE database is ***SIM.3.

That at the time that the deponent installed the new SIM card ***SIM.2 she received

two text messages (SMS) from SANTEVIÓS, with an SMS code to transfer

5,000 euros and an SMS from INFOSNET with an SMS code to transfer

reference of 5000 euros.

That the demonstrator, once the change request form is delivered

note that the email ***EMAIL ACCOUNT.1 does not apply

with the email provided to ORANGE. That the email you provided is ***ACCOUNT

MAIL.2(…)

That the protester gets in touch with ORANGE by phone through the

1470 and they inform ORANGE that two calls were made, one to change

change the email and another to request the duplicate of the SIM card, call

calls that were made on 07/22/20219, one at 2:00 p.m. and the other at

19:15 hours stating the number of the latter ***NUMBER.1.

That from the ORANGE store they enter the user profile and it is observed that

there are five calls to the telephone number ***TELÉFONO.2 that corresponds

to Santander's online banking (...)

That the protester examines the movements of her three bank accounts and

of his two cards and observe:

Which unknown author(s) had made a transfer of the VISA card

***VISA.1 for the amounts of 700 and 500 euros to the account ***ACCOUNT.1 (Ban-

co Popular) being the mirror account of the account ***ACCOUNT.2 (B. Santander).

The protester realizes that on July 22, 2019 unknown authors ten

A new VISA credit card with ***VISA.2 numbering was registered.

What unknown author(s) carry out a transfer of the card ***VISA.2 of 5000

euros to the bank account numbered ***ACCOUNT.3 (Banco Popular) being the

mirror account of account ***ACCOUNT.4 (B. Santander).

Which unknown author(s) made three transfers from his bank account

***ACCOUNT.5, (...) were 1000 euros each, sent to the accounts

***ACCOUNT.6 (EVO BANK); ***ACCOUNT.7 (EVO BANK) and ***ACCOUNT.8

(OPEN BANK) that for each of these transfers they charge the amount

of 6 euros.

Which unknown author(s) make a transfer from the account

***ACCOUNT.3(...) to account ***ACCOUNT.8 (OPEN BANK) for the amount of

250 euros, including a charge of 6 euros for expenses.

What unknown author/s of the account numbered ***ACCOUNT.1 (...) rea-

Three transfers were made, the first being for the amount of 5,000 euros to the

account ***ACCOUNT.6 (EVO BANK). A second transfer of 250 euros to

account ***CUENTA.8 (OPEN BANK), a third transfer of 250 euros to

the account ***ACCOUNT.8 (OPEN BANK). (…)

There is a "Request for changes in the Postpaid mobile communications service"

with a contact date of July 23, 2019, in which it appears in the "Data of the

Customer", the email of the impersonating person "***MAIL ACCOUNT.1" and in the

"Data of the Contracted Services" the new assigned SIM card number

***SIM.2.

There is a list of calls made from said SIM to the telephone line of the San-

tander ***TELÉFONO.2, and a summary of the transfers and deposits made without

Your consent.

C.C.C.: (…)

Concept

Immediate transfer in favor of Juan

Immediate transfer in favor of Juan

Immediate transfer in favor of Juan

C.C.C.: (…)

Concept

Deposit account from cards

Immediate transfer in favor of Lil

C.C.C.: (…)

Concept

Immediate transfer in favor of Juan

Immediate transfer in favor of Hugo

Immediate transfer in favor of Hugo

Deposit account from cards

Deposit account from cards

Date

07/22/2019

07/23/2019

07/23/2019

Date

07/23/2019

07/23/2019

Date

07/22/2019

07/23/2019

07/23/2019

07/23/2019

07/23/2019

Amount

1,006.00

1,006.00

1,006.00

Amount

5,000.00

256.00

Amount

5,006.00

256.00

256.00

700.00

500.00

In relation to this claim, ORANGE confirmed to this Agency that the card

SIM was acquired (...) and it was activated through (...) on July 22,

2019 at 6:52 p.m. The activation, he affirms, is carried out (...) in breach of the guidelines

procedures established by ORANGE to verify the identity of the client.

FOURTH: On June 5, 2020, a claim was received by this Agency

tion made by the complaining party two (file with reference number E/

05031/2020), directed against ORANGE, after being issued on January 8, 2020, a

duplicate of the SIM card of the line ***TELÉFONO.3, in favor of a third person.

na other than the owner of the line -the claimant party two-.

The facts were denounced before the General Directorate of the National Police in the

dependencies of San Andrés (Murcia), on January 9, 2020, with identification number

certified XXX/YY, with the following tenor:

“That on the day of the date the complainant's wife receives an SMS which informs her

way that through the number of the decedent has requested a duplicate card-

ta of your phone number.

That the declarant states that he has not authorized such an operation with his number by

so he contacts his phone company, ORANGE, to confirm-

dole this the processing of the duplicate, alleging that it may have been a mistake

by ORANGE.

That the declarant at that time realizes that he does not have coverage in

your mobile phone.

Who decides to check their bank accounts realizing that they have suspended

brought 300 euros from an ATM located at the scene without authorization

tion. (…)”

In relation to this claim, ORANGE confirmed to this Agency that the duplicate

The SIM card request was made on 01/08/2020 from (...) and was obtained through the

contribution of manipulated documentation among which was (...). It was detected

ted the same day of its activation, 01/08/2020, when associating the activation of the line

***PHONE.3 to IMEI ***IMEI.3, which was included in (...) used by the

Risk Analysis Group.

There is evidence provided (...) with which the supplanting person identified himself as the substitute party.

crying two, and it is observed (...) in different fields:

- (...).

- (...).

It is verified that some documents are missing to be delivered according to the ORANGE protocol:

- (...).

- (...).

FIFTH: The two complaints filed affect clients of the ORANGE brand.

GE.

SIXTH: ORANGE has a request and action management model for this brand.

Activation of duplicate SIM cards that it lends through (...).

.- (…)

.- (…)

(...):

(...):

- (…)

- (…)

- (…)

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

(...):

- (…)

- (…)

- (…)

- (…)

SEVENTH: ORANGE has a system (...)

(…)

(…)

(…)

(…)

(…)

(…)

(…)

(…)

(…)

(…)

(…)

(...):

- (...).

- (...).

- (...):

- (...).

- (...).

(...):

- (...):

- (...):

C/ Jorge Juan, 6

28001 – Madrid

either (…).

either (…).

either (…).

either (…).

either (…).

either (…).

either (…).

either (…).

either (…).

48/99

www.aepd.es

sedeagpd.gob.es

49/99

- (…)

(...):

either (…).

either (…).

either (…).

either (…).

either (…).

either (…).

either (…).

(...).

EIGHTH: (...):

either (…).

(...).

As (...) reports the following:

 (…).

 (…).

 (…).

 (…).

Regarding the (...) reports:

 (…).

NINTH: (...), ORANGE collects the following information:

(...).

(...).

Point 1 called (...) contains the following specifications:

- (...).

- (...).

- (...):

- (...):

- (…)

- (…)

- (…)

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

50/99

- (...):

- (…)

- (…)

(…)

- (…)

- (...).

- (...).

- (...).

- (…)

- (...).

- (...).

- (...).

As for the (...) ORANGE includes the following specifications:

• (…)

• (…).

TENTH: (...):

(...).

(...).

(...).

(...).

It is noted that the image of the first DNIe (issued since 2006) is not included.

until the end of 2015) available on the website of the General Police Directorate:

https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?

page=REF_3004&id_menu=51

It is verified that the new DNIe is not included among the identification documents

4.0, operational since the entry into force of EU Regulation 2019/1157 of the Parliament

European and Council of June 20, 2019, on the reinforcement of the security of

the identity documents of the citizens of the Union and of the documents of

residence issued to citizens of the Union and to members of their families who

exercise their right to free movement, that is, from August 2, 2021.

ELEVENTH: ORANGE is part of the Spanish Association for Digitization and

participates in the "Secure Digital Identity (IDS)" project, which aims -among

others, protect against fraud and cyberattacks and the defense of the privacy of the

data.

It actively participates in the proposal of different driving projects and in the development

llo of applications that guarantee the IDS.

(…)

TWELFTH: ORANGE has adopted a series of actions to prevent SIM

Swapping:

either (…).

either (…).

either (…).

either (…).

either (…).

either (…).

either (…).

either (…).

either (…)

either (…).

either (…).

THIRTEENTH: There is evidence of the dissemination of several "Internal Memoranda" issued by

the Fraud Department:

Contents

(…)

(…)

(…)

(…)

(…)

Date

09/11/2019

09/11/2019

09/12/2019

9/10/2019

12/19/2019

FOURTEENTH: There is a recording related to the activation of a request for

duplication of SIM card on the line ***TELÉFONO.4 made on date

04/22/2019. The activation of the SIM card is requested through (...) without the agent

business properly applies the protocol (...). There is no record of sending the

correspondent (…).

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 the provisions of articles 47, 48, 64.2 and 68.1 of the LOPDGDD, the

Director of the AEPD is competent to initiate and resolve this procedure.

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 by ORANGE in relation to the facts under 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.

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

ORANGE, identifying the vulnerabilities that may exist in the procedures

implemented operations, to detect the causes for which they could be pro-

ducting 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:

“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 ORANGE has a policy of

security in which the way of acting before data processing is established

personnel necessary for the issuance of duplicate cards. Nevertheless,

It was also proven that adequate security had not been guaranteed in the

processing of personal data, taking into account the result produced by the su-

identity plantation.

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 ORANGE, it was verified, among others, the implementation of a

most effective model for avoiding the risk of identity theft, the review, re-
strength and improvement of the security measures applied in the different channels
to ensure the identification and delivery procedure of the SIM card, with the
in order to prevent the materialization of fraud. Also, the immediate reaction to
the facts described and the capacity of the operator to demonstrate its compliance.
For all 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.
Now, it has been proven that the measures implemented by ORANGE were
sufficient and not only because it has been exceeded and the transfer of data per-
sound to a third party.
In a non-exhaustive manner and by way of example, we will focus on the deficient confi-
guration of the existing controls in the information systems that did not reflect
the traceability of the change produced in the personal data of the client (address of
email -claimant party one-).
Or for example, the fact that the face-to-face route is determined as a priority channel
for the request of SIM duplicates. However, ORANGE (…). If an operator
establishes a certain measure such as the one exposed, of prevalence of a certain
channel, the circumstances to avoid the measure should be controlled, since
otherwise, the implemented security policy is being distorted.
Also, if there are (...), it would be desirable for the system not to allow continuation with

the SIM change process if (...). ORANGE argues that in the case of the claimant

two, when dealing with (...), when previously, in the instruction of the procedure

lie has confirmed otherwise:

(...):

- (…)

- (…)

- (…)

- (…)

- (…)

- (…)

- (...).

- (…)

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 claimant two in which (...).

In addition, the (...) does not include the image of the first DNIe (issued from

2006 until the end of 2015) or the new DNIe 4.0.

Likewise, ORANGE contributed a (...):

(...).

(...).

This information does not correspond to what ORANGE alleges on July 27

of 2020, in which he confirms (…). Likewise, the information related to obtaining

the SIM (...) is not updated, since that access channel was eliminated on date 29

July 2019.

In short, to improve compliance with security policies, the instructions

transferred must be clear and up-to-date.

Likewise, ORANGE has not provided contractual documentation with the company, where

the conditions of delivery and the security guarantees in the identification

the client's. Let us remember that, although in the case of the complaining party one obtains

ga the SIM card (...) and in the case of the complaining party two, in person, the

Agency actions have been developed to investigate the entire procedure

shipping and delivery. Therefore, it would be advisable to include in the contracts the commitment

delivery of the SIM only upon prior verification of the identity of the

addressee and exclusively to him.

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

with different purposes (article 6.1 RGPD), and the imputation to ORANGE of the

responsibility for 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, functions

of 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.

It should be noted that ORANGE does not explain to what extent your rights are affected.

defense and procedural rights for subsuming the facts in article 5.1 f) and not

in article 6.1 of the RGPD.

It argues that the Agency has not justified the reason why it considers that it incurs the

infringement of article 5.1.f) RGPD.

However, the AEPD has motivated with a brief reference to facts and grounds

of law, as required by article 35.1.h) of the LPACAP, the basis for its decision

cision. Likewise, it 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, for

Therefore, it can plead helplessness. He has been able to allege and contribute to the procedure everything

that to its right has agreed, 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 ORANGE maintains,

Article 85.3 a) of the GDPR would also apply.

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 and under certain circumstances, you can make

the acts of patrimonial disposal that you want. Therefore, it is the responsibility of the

operator to establish requirements that, although a quick reading may seem

be very strict, a much more careful reading has shown that it is not

were. With which, the scam or impersonation, which apparently could seem complete

and difficult, it is observed that it has not been so difficult due to the inadequacy of the measures

security measures when it comes to monitoring who is the owner of the SIM card or the person

this authorized the one requesting 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»: any information about an identified natural person or

identifiable ("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, autho-

public authority, service or other body that, alone or jointly with others, determines the

purposes and means of treatment; whether the law of the Union or of the Member States

determines the purposes and means of the treatment, the controller or the criteria

Specific criteria for their appointment may be established by Union Law or

of the Member States”

8) “in charge of the treatment” or “in charge”: the natural or legal person, authorized

public entity, service or other body that processes personal data on behalf of the res-

responsible for the treatment;

ORANGE, is responsible for the data processing referred to in the foregoing.

exposed, since according to the definition of article 4.7 of the RGPD it is the

that determines the purpose and means of the treatments carried out with the purposes

indicated in its Privacy Policy, as has been proven in the Proceedings.

bados, section First.

Likewise, the issuance of a duplicate SIM card supposes the treatment of the damages

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

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

by an identifier (article 4.1) of the RGPD).

In this sense, it should be clarified that, inside the mobile terminal, the card is inserted

SIM. It is a smart card, in physical format and of reduced dimensions, which contains

It has a chip in which the service key of the subscriber or subscriber is stored.

gives to identify itself to the network, that is, the customer's mobile phone number

MSISDN (Mobile Station Integrated 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 holder.

ORANGE adduces a series of nuances regarding the data subject to treatment.

unto

The treatment activity questioned has been the request and action management model.

Activation of duplicate SIM cards that you lend through the face-to-face channel (from

points of sale) and the online channel (through the Mi Orange App and the area of

client/e-Care), not the treatments carried out by third parties or other entities.

des, such as the financial ones, which it invokes in the allegations.

He reasons that there is no evidence that the IMSI has been dealt with. In this sense, the IMSI in the me-

measure that makes it possible to single out an individual, and therefore identify him, must be considered

data of a personal nature in accordance with article 4.1 of the RGPD.

It is worth mentioning the Judgment of the Court of Justice of the European Union

(STJUE) of October 19, 2016 Case C-582/14, which considers that even the di-

dynamic IP address must be considered personal data to the extent that

the service provider has the means to know the identity of the holder of that di-

dynamic IP address.

Or the most recent STJUE of June 17, 2021 Case C-579/19 that in its section

102 recalls that "(…) A dynamic IP address registered by a service provider

online media services on the occasion of the consultation by a person of an In-

internet that that provider makes accessible to the public constitutes with respect to said pro-

sees personal data within the meaning of article 4, point 1, of the Regulation

2016/679, when he has legal means that allow him to identify the person.

interested person thanks to the additional information available to the provider of ac-

Internet access of that person (...).

This means that as long as there is the possibility of carrying out the identification, we will be

We are dealing with personal data.

This consideration is important in relation to the specific case, as remember

that the dynamic IP address is one that changes from time to time, for example

by changes in the network, or by the reboot of the device with which the service provider

services the connection provides, as opposed to the static IP address that

it is always the same. In any case, the company that provides the telecommunications service

cations knows at all times which is the dynamic IP through which the

ce the connection in relation to each of its clients.

If the CJEU considers said dynamic IP address to be personal data, "which changes every

certain time" it is logical to consider that the IMSI, which have a permanent character and

from which is derived, therefore, a better individualization of the user and also his identity.

fication, may also have such consideration.

Likewise, the Judgment of the Provincial Court (SAP) of Barcelona no. 390/2019

of May 30, provides: "However, the identity of the holder of the SIM card, or

which is the same, the identity of the holder of the telephone number associated with said card-

ta, does not constitute traffic data derived from telephone communications or a

data that affects the communication itself. There is no doubt that it is a fact

personal information regarding the privacy of the person covered by art. 18.1 EC."

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

identifies 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 Directive 95/46

understands, in accordance with the definition contained in article 2, letter a), of said Directive

goes "any information about an identified or identifiable natural person". This con-

The concept undoubtedly includes the name of a person next to their telephone number or

other information relating to your working conditions or your hobbies'.

Also, this opinion is singled out in relation to mobile telephony devices

that allow the location of the interested party, in Opinion 13/2011 on services

of geolocation in smart mobile devices (document WP185):

"Smart mobile devices. Smart mobile devices are

are inextricably linked to natural persons. Normally there is

direct and indirect identification. First of all, the operators of

telecommunications that provide access to the mobile Internet and through

GSM network normally have a record with the name, address and

the bank details of each customer, together with several unique numbers of the

device, such as IMEI and IMSI. (…)"

In fact, the clause “2.1.2. SIM card” of the general conditions of the services

ORANGE services, has: The SIM Card is a card that can be physical or digital

"eSIM" and that allows to identify the Service subscribed by the Client and the contracted line

in order to provide you with the Mobile Service. Hereinafter, the terms “SIM” or “Card

SIM” may be understood to refer indistinctly to the physical SIM Card or eSIM.

Likewise, ORANGE in the document (...) provided on July 27, 2020, in-

form:

“(…).”

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

SIM card (Subscriber Identity Module) that uniquely and uniquely identifies

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

subject to data protection regulations.

FIFTH: Allegations adduced to the Resolution Proposal.

We proceed to respond to them according to the order set out by ORANGE:

FIRST: INFRINGEMENT.

Regarding this allegation, we refer to the provisions of the Third FD of this Re-

solution.

SECOND: PROCESSING OF PERSONAL DATA AND RESPONSIBLE FOR THE TREATMENT

TREATMENT.

We refer to the previous FD.

THIRD: ALLEGATIONS ADUCTED.

1. PRIOR ALLEGATION. - EXISTENCE OF A WG ON DUPLICATION OF

SIM CARDS LEADED BY THE AEPD.

It alleges a bankruptcy in the legitimate trust deposited in the Agency by the

opening of this procedure.

It is not possible to appreciate the violation of the principle of legitimate expectations, collected

in article 3.1.e) of the LRJSP, a principle that, as the jurisprudence has reiterated,

dence - SSTS of December 28, 2012 (Rec. 273/2009), July 3, 2013

(Rec. 2511/2011), among many others- "it cannot be invoked to create, maintain

have or extend, in the field of public law, situations contrary to the

legal system", being the alleged plaintiff responsible for the infractions

tions appreciated in the initiation agreement, in accordance with article 28.1 of the LR-

JSP.

In relation to this principle, the Judgment of the National High Court (SAN),

of April 29, 2019, RJCA 2019\449, indicates: In accordance with what was declared by the an-

aforementioned judgment of July 6, 2012 (RJ 2012, 7760) the principle

of legitimate expectations means 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 based on which the particular

res have made certain decisions. (...) as stated in the sen-

judgment July 3, 2012 (RJ 2012, 11345) (appeal 6558/2010): "(...) The pro-

protection of legitimate expectations does not cover any type of psychological conviction

subjective logic in particular, being only susceptible to protection

that <confidence> on concrete aspects, which is based on signs or

external data produced by the Administration sufficiently conclusive

tes..." But from the very decisions of this Chamber, it must be concluded in a

important and relevant element to configure the legitimate trust, to save

ber, that the concrete action that is expected in that trust is in accordance

to the Legal System (last-cited judgment), that is, it is necessary that the

action of the Administration, with its conduct, induces the company "to

believe that the action that he develops is lawful and adequate in law"

(judgment of July 3, 2012, issued in appeal 6558/2010). In that

In the same sense, it has been declared that it cannot rely on legitimate trust.

tima "the mere expectation of an invariability of circumstances", as

declared in the judgment of March 22, 2012 (appeal 2998/2008), in the

that it is concluded that a behavior cannot be irreversibly maintained

which is considered unfair.

Precisely because it is a generalized and recurring problem,

it was considered opportune to carry out preliminary investigation actions.

In the Fourth Precedent we made reference to the three requirements of

training aimed at ORANGE on different dates.

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.

It should be noted that article 53 of the LOPDGDD determines the "Scope of

research activity":

1. Those who develop the research activity may collect the information

precise instructions for the performance of their duties, carry out inspections

nes, require the exhibition or sending of the necessary documents and data,

examine them in the place where they are deposited or where they are

come out the treatments, get a copy of them, inspect the equipment

physical and logical and require the execution of treatments and programs or procedures

Treatment management and support procedures subject to investigation. (…)

Thus, the Agency can carry out the investigations it deems appropriate

(Article 67 of the LOPDGDD), after which you can decide to initiate an ex officio

penalty procedure (article 68 of the LOPDGDD). We are not using

using no pretext, as alluded to by -news in the press-, to justify our

action, but before the application of the general principles that govern the

act of public administrations, article 3.1. of the LRJSP: The Admi-

Public administrations objectively serve the general interests and act

in accordance with the principles of efficiency, hierarchy, decentralization,

concentration and coordination, with full submission to the Constitution, to the

Law and the Right.

ORANGE reasons that there are other corrective mechanisms, however, in-

we serve, the LOPDGDD regulates in Title VIII the "Procedures in case of

possible violation of data protection regulations" and specifically, the

Article 64.2 provides that, when the purpose of the procedure is to determine

mination of the possible existence of an infraction, will be initiated by

initiation agreement adopted on its own initiative or as a consequence of re-

claim (in the case analyzed, there have been two claims of

affected).

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Likewise, article 109.2 of the LRJSP provides regarding the Authorities

Independent Administrative Companies that will act, in the development of their activity

and for the fulfillment of its purposes, regardless of any interest

business or commercial.

In short, the participation of ORANGE in the WG does not modify the responsibility

ity now imputed to him. Therefore, due to the fact that there is participation

do in a GT whose objective is to deal with such a specific criminal activity

("SIM Swapping"), does not prevent that once an infraction is verified, it must

be sanctioned

2. FIRST ARGUMENT. - INCORRECTION AND LACK OF ACCURACY IN THE

APPRECIATIONS ON DUPLICATE FRAUD.

The Agency has at no time stated that the SIM allows access to the

IMEI. We only refer to it for the purpose of clarifying that both one and the other

(IME and IMSI) have the status of personal data in accordance with the definition of the

article 4.1 of the RGPD.

In the opinion of ORANGE, no personal information has been accessed other than

the one provided by the supplanters. The Agency disagrees with this argument,

because, according to ORANGE itself in the document “Information and management

SIM cards”, the SIM card “stores all the information about the telephone line

the client's; is the element that supports the line and the telephone number and allows the

terminal access to the network.

According to LGTEL, electronic communications services are considered

tion of “services of general interest”. Let us not forget that through these services

connectivity is guaranteed to such important services as fixed telephony, mobile

or Internet access. (article 2.1 LGTEL)

Likewise, the obligatory respect for the protection of the personal data of the users

riors of this sector (article 41 LGTEL) also appears within the "obligations

of a public nature” applicable to the electronic communications sector (Title

III, chapter III).

41.1. The operators that exploit public networks of electronic communications

nicas or that provide electronic communications services available to the

public, including public communications networks that support

identification and data collection positives, they must adopt the measures

adequate technical and management measures to preserve safety on the farm.

tion of its network or in the provision of its services, in order to guarantee the

protection of personal data.

Considers that the Agency mixes concepts, insofar as the key refers to

taken by the bank (possession factor) does not have the status of personal data and does not

may be considered a breach of security or confidentiality.

In these strong customer authentication systems, in accordance with article 4.30

of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November

November 2015 on payment services in the internal market and by which

Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU)

No 1093/2010 and Directive 2007/64/EC (hereinafter PSD2 Directive) is repealed,

authentication is based on the use of two or more categorized elements

as knowledge (something that only the user knows), possession (something that only

see the user) and inherence (something that is the user). These elements or factors

are independent of each other and, therefore, the violation of one does not compromise the

reliability of others.

The basis is very simple: the more elements you have to verify the

identity of the user, the more secure the transaction. Now, if those elements

are not applied properly, the operation fails.

Let us remember that, in these cases, the impersonator must first enter

the username and password or password in the application or on the provider's website

payment service or online banking.

Second, to complete the transaction or electronic management you want

perform, the impersonator will receive, normally through an SMS, an alphanumeric code

verification number on the mobile phone linked to that profile. This code has

a limited temporary validity and is of a single use, that is, it is only generated

for that specific transaction and for a limited time. Once you have entered the

verification code, the transaction would be made and completed.

It is assumed 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,

tion via SMS, your identity would be doubly authenticated.

Therefore, it would not be enough for the impersonators to be able to commit the fraud with co-

know the username and password with which the victim identifies, but it will be necessary

They must intercept said confirmation code.

Consequently, in order to carry out a transfer, transaction or purchase

consented, that is, to carry out the computer fraud, the cybercriminal de-

You will need to illegitimately access the verification codes associated with each of the

those operations sent by the bank through SMS and the way

The most common way to do this is by obtaining a duplicate of the card.

SIM.

In fact, ORANGE, in the document cataloged as “(…) (SIM Swapping)”

He says:

"1(…)."

Therefore, it is necessary to execute two completely different actions but

complementary to each other.

First of all, you have to obtain the access data for online banking or providers.

payment provider owned by the person to be defrauded, if we focus on the search

of wealth enrichment.

And, secondly, you will have to obtain the duplicate of the SIM card owned by

of the person to defraud in order to get hold of the confirmation SMS

that the client will receive in his mobile terminal as two-factor authentication. The

Authentication systems are, in accordance with European legislation, procedures that

allow the payment service provider to verify the identity of the user of

a payment service or the validity of the use of a certain payment instrument.

payment, including the use of the user's personalized security credentials.

river (article 4. 29 of the PSD2 Directive).

Well, in the last of these actions -obtaining the duplicate-, it is where

have focused on the facts that are the subject of this proceeding and not on those that occurred in the

first phase, which remain outside the responsibility imputed to ORAN-

GE.

He refers to a Guide on Digital Identity and to the responses of the EBA, which questioned

They guarantee the security of SMS to confirm banking operations. Nevertheless,

the security measures applied to online banking operations regarding

to the treatments carried out by financial entities, are not subject to analysis

in this file.

3. SECOND ARGUMENT. - UNFOUNDED GENERALIZATION OF CONSE-

NEGATIVE ACCOUNTS ASSOCIATED WITH THE ISSUANCE OF THE DUPLICATE.

ORANGE reiterates the allegations made previously, in respect of which

the AEPD reproduces what it already determined in the Resolution Proposal.

We already indicated that we upheld the allegation that the access

so to the duplicate does not provide direct access to the contacts stored in the

original SIM card, since, as it is a physical device, all

the data it contains and lost contacts on the card cannot be recovered

replaced SIM, unless they have been stored in environments associated with An-

droid or Apple, in which case the device must be synchronized with a certain

account to be able to restore them.

Regarding access to email, bank and other accounts.

In order to commit the criminal modality of SIM Swapping, in general,

It is necessary to execute two completely different but complementary actions.

you laugh with each other First of all, you have to obtain the access data for online banking.

line or payment provider owned by the person to be defrauded, if we focus on

the search for wealth enrichment. After that, the duplicate will have to be obtained.

ing of the SIM card owned by the person to be defrauded in order to

close with the confirmation SMS that the client will receive on his mobile terminal as

two-factor authentication.

When the criminal modality seeks patrimonial enrichment, it is necessary

take the two steps described above. However, when the

criminal modality seeks other purposes such as impersonating the person

sona on social networks, snatching private messages on social networks, becoming

with emails available on network servers, find out private data

of the person with the purpose of forcing him to execute certain actions... it is

that is, criminal actions constituting other criminal behaviors such as coercion

tions, crimes against privacy, crimes of threats, harassment, insults or slander,

the first action is not necessary, but with the simple obtaining of the duplicate

of the SIM card is enough. It is common for social networks or servers to

mail, in case of forgetting the password opt for fast mechanisms directed

two to obtaining a new password, such as sending a link

to the telephone line offered when the user signed up for it. With which,

when the offender has that telephone line with the duplicate of the card

SIM, you will receive in the terminal the possibility of creating a new password having free

thereby accessing social networks, instant messaging, web browsing,

cloud, emails... of that person, since the user is a relative data-

simple mind to find out.

In short, the rigor of the operator when it comes to monitoring who is the holder of

the SIM card or person authorized by him who requests the duplicate, should answer

adhere to strict requirements. It is not that the information referred to

it is not contained in the SIM card, but that, if in the process of issuing

tion of a duplicate SIM card does not adequately verify the identity of the

applicant, the operator would be facilitating identity theft.

The 2021 Report of the State Attorney General's Office dedicated to "Internal Crime"

formatica" dedicates in its point 8 a mention to the fraudulent actions online:

"In this brief review of online fraudulent actions, it is necessary to

the mention of behaviors that affect the telecommunications sector

tions in their different variants, and closely related to them, although the

damage is generated in online banking, commonly known as fraud.

of SIM Swapping, which is being used with alarming frequency in

the last years. The technique consists of circumventing the security measures

of banking entities by accessing the alphanumeric codes of

confirmation, single use, generated on the occasion of transactions

electronic and that are ordinarily communicated to clients through

of SMS messages. To do this, criminals previously obtain a

duplicate or a new SIM card in the name of your victim, either requested

taking it from the corresponding operator, simulating its identity,

either using a more elaborate methodology, as in the assumption

object of judicial investigation in Zamora, in which it took advantage with

that purpose a mobile repair shop. once they have

SIM card at your disposal, criminals are guaranteed reception

on your own device of the confirmation code of the fraudulent transaction

dulent and, ultimately, the possibility of making it effective in its be-

benefit, preventing it from being known at that time by the injured party or

harmed. This form of fraud has generated in recent years

multiple police investigations and the initiation of legal proceedings

specialties in different territories such as A Coruña and Valencia. Its effectiveness and

ease with which criminals achieve their illicit purposes has determined

undermined the adoption by telephone operators of specific measures

prevention measures and strengthening of the guarantees for the issuance of

tas cards or their duplicates."

ORANGE argues that its responsibility cannot extend beyond those

issues that fall under its scope of action and that there is no lack of diligence

agency, but rather performs these operations by requesting data from the person who supposedly

is its owner and even provide falsifications of public documents as a means

to overcome control measures.

Well, in the list of 20 cases of SIM duplicates reported/claimed

such as identity theft or fraudulent by customers, relating to the line

***TELEPHONE.4 made on 04/22/2019, the activation of the tar-

SIM card (...) that are included in the Security Policy (...).

At this time, and in response to the allegations made by ORANGE in re-

relationship with the list of the 20 cases collected we have to mean that as a result of

the two claims for identity fraud, which involved on the part of the respondent

responsible for processing the issuance of the customer's SIM card duplicate to a third party

zero (after which there have been serious economic damages to those affected) in-

investigate in depth the origin of the problem in order to find out if it was due to a

flaw in the privacy protection model. The focus is not on third parties

that they have surpassed the security policies, but on why they have surpassed them;

that is, it examines the condition, characteristics and adequacy of the policies cited

data protection regulations and the actions of the data controller

I lie about it. For this reason, the 20 cases related to duplicates of old SIM cards

nen to the case, showing the deficient application of the security policy.

Likewise, in the case of claimant one, the email address was changed

prior to the SIM request, without ORANGE being able to

accredit some evidence in their management systems about the controls that are

they went through for the change of the customer's email address.

In the case of claimant two, the documentation (...). He was not even asked

cited an additional control requirement (some question or some original documentation)

ginal) since it was provided (...).

In fact, the operator openly admits that the protocols were not complied with.

los, alluding to the deception suffered by the workers. The human factor, the obvious

possibility of making mistakes or being deceived, is one of the most important risks

always to be considered in relation to the determination of safety measures

security. The data controller must take into account human error as a

risk more than likely. Human errors are combated from the approach of

risks, analysis, planning, implementation and control of technical measures and

adequate and sufficient organizational

A criminal may attempt to deceive and cause human error, but it is the measures

adequate security measures who act as brakes.

As far as the criminals have failed to obtain personal data from

ORANGE, so there can be no question of non-compliance with protection measures.

tion, point out that access to the duplicate of a SIM card that makes identifiable to

its owner, responds to the definition of personal data in article 4.1) of the RGPD.

For all the above reasons, it has been considered that the procedures for the issuance of

SIM card applications required improvement in order to ensure

the security of customers' personal data effectively and in particular

cular, its custody, in order to prevent unauthorized access.

4. THIRD ARGUMENT. – SUITABILITY AND COMPLIANCE WITH THE MEASURES

PREVENTIVES IMPLEMENTED.

ORANGE reports the number of SIM changes made in 2019, (...), without

There has been no incident in the (...) of the cases. Consider, therefore,

that their protocols have proven to be effective.

However, this sanctioning procedure has had the objective of analyzing the

procedures followed to manage SIM change requests, certain

nating, where appropriate, the violation of the principle of data confidentiality

(in this case, the SIM card) treated by ORANGE as responsible

of treatment and if that violation has been the product of security measures

insufficient.

During 2019, ORANGE reports having provided (...) card duplicates

SIM.

As we have indicated before, the Agency has focused, not only on the

that third parties have overcome the security measures implemented by

ORANGE, but on why they have overcome them; that is, the condition is examined,

characteristics and adequacy of the measures cited to the regulations for the protection of

data and the action of the data controller in this regard.

Regarding the risk approach, it should be noted that the Agency does not intend to require

at no time a zero risk. But the GDPR itself indicates that the measures

must be adequate, according to the foreseeable risk. And the RGPD neither

does not make any reference to the percentages of materialization of the risk from the

which may or may not be considered negligible for the purposes of not considering it

infraction or lack of diligence.

It is considered that it is more than proven that the practice of this type of fraud,

like the one analyzed here, is a frequent practice and, therefore, the operators

must have appropriate measures to ensure that they do not unduly facilitate

mind a SIM card to someone who is not the legitimate owner. Hence, from the analysis of

documentation, it is concluded that the measures adopted have not been adequate.

give for this purpose.

ORANGE alleges a breach of the strict liability principle in the

sanctioning vetoed by our legal system.

In this regard, this Agency has already informed in the Background of the Start-up Agreement and

in the Resolution Proposal, that in addition to the two claims, the SGID included

investigated the "fraudulent practices based on the generation of duplicate credit cards"

SIM cards without the consent of their legitimate owners in order to access information

confidential training for criminal purposes (known as “SIM Swapping”)” as

consequence of "news appearing in the media", as

it follows from the internal note of the director that appears in the file.

Therefore, the origin of the problem has been thoroughly investigated in order to ascertain

guar if there could be a flaw in the privacy protection model.

It is not true, as ORANGE pretends to show, that the cir-

circumstances -exclusively- of two specific cases, since, aside from these

complaints, has been directed to analyze whether the technical and organizational measures

adopted by ORANGE for the issuance of duplicate SIM cards to holders

telephone lines were appropriate to ensure the mitigation of

the possible risks to the fundamental rights and freedoms of the holders of

the lines.

The circumstances of the two cases in which a claim has been filed with

the AEPD have revealed the insufficiency of security measures

adopted by ORANGE, which also recognizes that such measures have been insufficient

patients in a total of (...) cases during the year 2019.

In addition, it must be taken into account that the seriousness of the proven facts is reflected

ma in the social alarm generated by the realization of these fraudulent practices,

without determining the number of claims filed.

ORANGE alleges that the overcoming of security measures by a third party does not

can determine by itself that they are not adequate or sufficient. Y

cites file E/05168/2021, in which a claim was filed after verifying

It should be noted that, despite having access to personal data by a third party,

unauthorized zero, a sufficient and appropriate level of diligence had been

do, even if the security measures implemented had been overcome.

In said file, the circumstances were different. It was a third party who is-

was making a series of queries and requests about the owner's line, due to

because it had the personal information of the claimant because of the link that

had united them. In the opinion of this Agency, the information that

can be obtained due to a link with the information that can be obtained by a ci-

berdelinquent For its part, the operator not only implemented measures to prevent

such situations occur in general, but also for the specific case. Y,

Lastly, that claim was filed in application of the principle of presumption of

innocence, which prevents imputing an administrative infraction when no

had evidence or indications from which the existence of an infraction is derived. The experience

tooth that is now resolved is different, in which -in addition to the two claims-

nes-, a series of cases reported by ORANGE itself have been verified, in

which has materialized access to (...) duplicate SIM cards in an in-

due, as a consequence of the lack of appropriate security measures

to avoid it.

ORANGE also cites file E/00536/2016 in which the identity is supplanted.

ability to modify the claimant's data on the ORANGE intranet. And adds

that the Agency considered that “the misuse or improper use through impersonation

of identity by a third party is not attributable to Orange, since it complied with

appropriate security measures" and that "despite the fact that there was illegal access,

The Agency concludes that: “No evidence has been accredited that would allow

so attribute to Orange a violation of the regulations on the protection of

data, to the extent that it acted diligently” and, consequently, files the

process".

In this file, a third party had improperly accessed the services

offered by ORANGE through the website and had made a series of

fraudulent orders of mobile terminals. Therefore, its purpose was to analyze

if the measures available to ORANGE to identify the person who carried out

The request from the terminals had been enough to understand that there was action.

acted with reasonable diligence. In this sense, it was considered that ORANGE used

a reasonable diligence since -precisely-, it adopted the necessary measures

to identify the person who made the request for the terminals (when requesting

username and password for the procedure) and that, as soon as he became aware of the claim,

tion, canceled the requested orders.

However, we are facing different assumptions, given that in file E/

00536/2016, only fraud takes the form of placing fraudulent orders.

slow mobile terminals, while in this procedure it is about facilitating

take a duplicate of a SIM card (personal data) to someone who is not its owner, which

leads, as has been repeatedly explained, to a loss of control of the

personal information.

It also cites file E/2723/2020, in which it states that it is considered that

ORANGE took the appropriate measures. However, the resolution of the aforementioned ex-

The petition at no time affirms that the measures adopted by ORANGE were

they were adequate. What it states is that: “the lack of rational evidence has been confirmed

them of the existence of an infraction (...), not proceeding, consequently, the

opening of a sanctioning procedure”. And this under the principle of presumption

innocence, according to which an administrative infraction cannot be imputed

when no evidence or indications have been obtained from which the existence

possession of an offence. The fact of stating that no evidence has been found

of infringement by ORANGE is very different from asserting that the measures

adopted by ORANGE were adequate, which is not the case in this file.

ORANGE also mentions the file E/06963/2020. In this, the Agency does not

admits to process the claim on claim of payment of invoices of telephone lines

contracted telephone companies using your personal data without consent, therefore

claim that the claim in question had been addressed, by blocking ORANGE the

contracted services and cancel the claimed debt.

Nor is it stated in that file that the measures available to ORANGE

were suitable. In fact, the aforementioned measures are not even analyzed.

In any case, the aforementioned resolution also provides "All this without prejudice to

that the Agency, applying the investigative and corrective powers that it os-

tenta, can carry out subsequent actions related to data processing

referred to in the complaint. This is, without prejudice to which, this Agency may in-

Find out about the procedure followed in general for this type of event. By

Therefore, even if in that specific case the claim had been inadmissible in

issue, this does not prevent the Agency from examining the security measures

that ORANGE has in order to prevent a third party from contracting telephone lines.

phone in your name without your consent.

For its part, ORANGE also mentions file E/05272/2018, in which

various workers spread images of clients suspected of having

brought objects via WhatsApp and, there being no indication that the entity had in-

fulfilled its obligations in compliance with the principles of integrity and confidentiality.

entiality, proceeded to agree on the filing of the proceedings.

In this regard, this Agency wishes to point out that the factual assumption is considerable-

mind different from the one analyzed in this sanctioning procedure. And that the fact

that in said file no reasonable indications of the existence

ence of a security breach in the treatment carried out by the person in charge of

treatment with respect to the data of its clients, this does not prevent that in this process

sanctioning procedure it had been proven that ORANGE has facilitated access

to fraudulently requested SIM card duplicates, as a consequence

consequence of having security measures that are not adequate for such

finish.

ORANGE also mentions file E/07129/2014, in which the AEPD archived

The procedure is based on the fact that it is not possible to determine the identity of the in-

offender, the principle of presumption of innocence prevents the imputation of an administrative

nistrativa when the existence of proof of identity has not been obtained and verified.

accrediting charge of the facts that motivate the imputation.

In this regard, it should be noted that, in said file, a claim is made for the

of a purchase on a website made, on your behalf, without the consent of the

claimant. First, the factual assumption is considerably different from the

analyzed now. And regarding the principle of presumption of innocence, we reiterate

that this principle prevents imputing an administrative infraction when there had not been

have obtained evidence or indications from which the existence of an infringement is derived,

question is that if it concurs in the analyzed case.

ORANGE cites file E/08205/2019, in which there was a security breach

security, in which names, surnames and other personal data of clients were leaked.

tes, reaching more than 1,300,000 affected. The Agency considered that the entity

defendant had the necessary technical and organizational measures to

address a breach such as the one that occurred and that it adopted the necessary additional measures.

ries to mitigate the impact and prevent the event from happening again in the future.

It should be noted that this assumption was about a hacker who had obtained

the database of users registered on a website and marketed through

see the deep web. And that during the investigation carried out, it was found that the

security measures that the data controller had were adequate

given to deal with an incident of these characteristics and that he had reacted in a

diligently in order to notify, communicate and minimize the impact and implement

take appropriate reasonable measures to prevent the recurrence of an incident in the future.

similar tooth. However, in addition to the assumption of fact being considerably

different from the assumption analyzed here, the fact that in said file it is

would have appreciated that the person responsible for treatment had the measures of

appropriate security, this does not prevent this sanctioning procedure from

verified that ORANGE facilitated access to duplicate SIM cards, without

ensure the identity of their holders.

Lastly, ORANGE mentions file E/05441/2018, in which the company

claimed suffers a security breach, where the attacker gains access

unauthorized way to a database of the claimed. The Agency indicates that the

gap has violated article 32 of the RGPD. However, it is noted that the claim

had implemented security measures that were, in principle, adequate

you give. Thus, it is considered that the actions of the respondent as responsible for the treatment

processing is in accordance with data protection regulations, archiving, obtaining

mind, the performances.

In this case, the attacker gained unauthorized access to a

claimant database. However, it was found that the defendant "had

implemented security measures that, in principle, were adequate to

ensure that personal data is not accessible by third parties and, as

It is stated in the facts, as soon as the attack was detected and confirmed by the

a series of additional security measures were immediately adopted.

in order to minimize the risks and extreme the difficulties for the acces-

so and information extraction". As stated above, in addition to

that the assumption of fact is considerably different from the assumption of analytic fraud.

lyzed, the fact that in said file it had been appreciated that the responsible

The treatment provider had the appropriate security measures for the case

concrete, it does not prevent that in this procedure it has been verified that ORANGE

had access routes to obtain duplicates (vending kiosks)

res or telephone activations) that favored identity theft.

ORANGE argues that the fact of allowing in certain si-

situations the use of non-face-to-face channels with no lack of diligence, as long as

so that any route is susceptible to being the object of fraud attempts.

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 establishing safety measures

strict security measures in a channel, if equivalent measures are not also established in

the rest of the channels, the global security is being reduced to that of the security channel.

minor security.

Regarding the freedom of managers to comply with security measures and

punctual non-compliance in these isolated cases, the imposition of penalties

for an amount of 300'00 euros, does not exempt the operator from its obligations with the

treatment managers.

From ORANGE's statements the conclusion seems to be drawn that it has no

no power of action to avoid these frauds or impersonations, since they attribute

All responsibility lies with third parties involved (in charge or supplanted-

beef). We do not agree with this conviction.

The concepts of controller and processor are not formal, but

functional and must attend to the specific case. The data controller is

from the moment you decide the purposes and means of treatment, not losing

such a condition the fact of leaving a certain margin of action to the person in charge of the traffic-

I lie. This is unquestionably expressed in 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. (…)

ORANGE must assess the (real) possibility of such a situation occurring and it is its

obligation to implement measures to avoid this type of situation or, at least, the quickly detect. Consider all these supposed deviations from the proto-Colos established by ORANGE as mere specific facts before which no additional actions are carried out to avoid them, it supposes not acting with due diligence and that is why it is considered that ORANGE has violated the obligation guarantee the confidentiality of personal data in the event here analyzed, as a consequence of lacking, precisely, the security measures suitable for this purpose.

Nor has this Agency required the "full monitoring of employees", as as stated by ORANGE. It simply requires that some measures be implemented of security according to the risk that exists that the agents do not comply with the measures provided by ORANGE, among others.

ORANGE states that (…). However, the mere fact (...) to verify the activity effective protection of users and adopt new measures, it cannot be considered as a sufficient and adequate measure for the aforementioned purposes. Lastly, you have to

Remember that this is not the only security measure that is analyzed or the only one that could be used to ensure the confidentiality of personal data in question.

Therefore, in addition to the security measures implemented after the commission of the Proven Facts and that are valued positively by the Agency cia, the infringement is considered proven. For all of the above, the infringement

imputed is the one provided for in article 5.1.f) of the RGPD.

Lastly, ORANGE indicates that “the nature of the fundamental right of the right to data protection does not eliminate the need to examine the diligence displayed given by ORANGE, nor the consideration of the tiny percentage of incidents that have occurred in the SIM card duplication processes. All the activity of the AEPD is about a fundamental right, so that argument is not valid to support the proposed sanction.

In this regard, make several nuances.

In the first place, the AEPD also exercises functions related to the rights digital rights (articles 89 to 94 of the LOPDGDD).

Secondly, the exercise of the sanctioning power has been carried out prior administrative procedure, accompanied by due guarantees, and has led to determine the Facts, prove guilt and graduate the administrative response tive. This graduation has not been made apart from the concurrent circumstances, but as a manifestation and requirement of the principle of transparency (article 3.1.c) LRJSP) and the right to good administration (article 41 of the Charter of Fundamental Rights of the EU), the facts have been treated impartially and equitably, motivating the final decision at all times.

Therefore, the Agency has limited itself to analyzing the circumstances of the case decree in order to identify the existence of indications or evidence (or not) of infringement tion in its field of competence. And as a consequence, it has considered proven that ORANGE has violated one of the principles relating to processing (article 5.1.f) GDPR).

5. FOURTH ARGUMENT. – DILIGENT PERFORMANCE BY ORANGE.

He invokes a total defenselessness, because despite the fact that he has managed to prove the compliance with his duty of diligence and being recognized, is subject to a sanction

tion for an unspecified reason.

The Agency has scrupulously respected the procedure, allowing ORAN-

GE the exercise of its right to effective protection, since in this proceeding

The principles of bilaterality, contradiction and equality of rights have been respected.

weapons as required by the reiterated doctrine of the Constitutional Court on the

right to effective judicial protection that (Valga for all the Judgment 220/2002 of

25 Nov. 2002, Rec. 5497/1999) “3. This Court has repeatedly stated

that the right to effective judicial protection without defenselessness, which is recognized in

the art. 24.1 CE, guarantees the right to access the process and legal resources-

established in conditions of being able to be heard and exercise the defense of the

legitimate rights and interests in a procedure in which the principles of

principles of bilaterality, contradiction and equality of procedural weapons, (...)

(SSTC 167/1992, of 26 Oct.; 103/1993, of 22 Mar.; 316/1993, of 25

Oct.; 317/1993, of Oct. 25; 334/1993, of Nov. 15; 108/1994, of Apr. 11; 186/1997,

from Nov 10; 153/2001, of July 2; 158/2001, of July 2).

The STC 86/1997, of 22 Apr., FJ 1, says: "the defenselessness must be material, and not

merely formal, which implies that this formal defect has been detrimental

real and effective price for the defendant in his possibilities of defense (STC

43/1989, 101/1990, 6/1992 and 105/1995, among others)”; in this sense, ORANGE,

at all times he has had knowledge of the facts imputed to him, the possible

ble infractions of which the facts are constitutive, has been able to allege as to

his law has deemed it appropriate and has been able to request the evidence and provide the documents that he has considered in his defense throughout the investigation of the case.

sanctioning procedure and, which have been analyzed and taken into consideration

as reflected in the Motion for a Resolution against which he has also presented-

the appropriate allegations that are being analyzed in this Resolution

tion, therefore, we reject the alleged allegation.

Likewise, far from ORANGE's claim that the paragraphs transcribed in the

Motion for a Resolution reveals an unsolvable contradiction,

certify that the Agency has scrupulously respected the principles of the procedure

sanctioning procedure and more specifically the right to defense of ORANGE.

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), which

which means that there must be some kind of fraud or guilt. As the STS says

of January 23, 1998, "...we can speak of a decided line of jurisprudence

that rejects in the sanctioning scope of the Administration the objective responsibility

tive, 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 guilt can include

refer to the principles of legality and prohibition of excess (article 25 of the

Constitution) or the requirements inherent to the rule of law".

Lack of diligence in implementing security measures at source

adequate constitutes the element of culpability.

Let us remember that clients -individuals or legal entities- sign contracts

fords with ORANGE for the provision of certain services that are submitted

to some privacy clauses contained in the Privacy Annex in accordance with

puts clause 13.1 of the "General Conditions of ORANGE Services".

For example, clause 8 of the current Privacy Policy says:

“8. Security measures

Information security is one of our firm commitments and

in compliance with current legislation ORANGE will process the data of the

User at all times in an absolutely confidential manner and keep

complying with the mandatory duty of secrecy with respect to them, adopting the

effect the security measures of a technical and organizational nature necessary

that guarantee the security of your data and avoid its alteration, loss,

damage, treatment or unauthorized access, taking into account the state of the

technology, the nature of the stored data and the risks to which it is

so exposed.”

Therefore, just as customers are required to comply with the obligations

tions stipulated in the contracts signed with the operator, from this, the

compliance with the obligations that in terms of security and confidentiality

compete.

In terms of due diligence, we acknowledge that ORANGE has acted subsequently

mind diligently when minimizing the impact to those potentially affected

implementing new security measures to prevent the recurrence of incidents

thousands in the future.

Certainly, the principle of responsibility established in article 28 of the LRJSP,

provides that: "They may only be sanctioned for acts constituting an infraction

natural and legal persons, as well as, when a Law recommends them

know capacity to act, affected groups, unions and entities without
legal personality and independent or autonomous estates, which result
responsible for them by way of fraud or negligence.”
However, the mode of attribution of liability to legal persons is not
corresponds to the willful or reckless forms of guilt that are im-
putable to human behavior. So, in the case of offenses committed
by legal persons, although the element of culpability must be present.
this is necessarily applied differently from the way it is applied to
physical persons.
According to STC 246/1991 "(...) this different construction of the imputability of the
authorship of the infringement of the legal person arises from the very nature of fiction
law to which these subjects respond. The volitional element is lacking in them.
strict compliance, but not the ability to break the rules to which they are subject.
Capacity for infringement and, therefore, direct blame that derives from the good ju-
protected by the rule that is violated and the need for such protection
is really effective and for the risk that, consequently, the person must assume
that is subject to compliance with said rule" (in this sense STS of
November 24, 2011, Rec 258/2009).
To the above must be added, following the judgment of January 23, 1998, par-
cially transcribed in the SSTS of October 9, 2009, Rec 5285/2005, and of 23
of October 2010, Rec 1067/2006, that "although the culpability of the conduct
must also be tested, must be considered in order to assume the
corresponding charge, which ordinarily the volitional and cognitive elements
necessary to appreciate it are part of the typical behavior tested, and that
its exclusion requires proof of the absence of such elements, or in its ver-
normative intent, that the diligence that was required by the person who claims

its non-existence; not enough, in short, to exculpate behavior

typically unlawful the invocation of the absence of fault".

Consequently, the lack of guilt is dismissed. ultimate responsibility

on the treatment continues to be attributed to the person in charge, who is the one who determines

the existence of the treatment and its purpose. Let us remember that, in general

The operators treat the data of their clients under the provisions of the article

6.1 b) of the RGPD, as it is considered a necessary treatment for the execution of

a contract to which the interested party is a party (…).

In this sense, ORANGE has a network of commercials, points of sale and

distributors approved through a distribution contract to offer the

ORANGE services. Among these services offered from its points of sale,

is the realization of duplicates of SIM cards corresponding to a line of

mobile telephony.

Let us remember that in the case of the claimant one, it was modified in the file of

customer the contact email that was previously stated (...). Subsequently, it was observed

had the issuance of a duplicate SIM card, even having reported (...)

in any procedure with the operator. And finally, there is the telephone activation

SIM card without sending a (...) to any of the lines associated with the contract

of the complaining party, (...).

As for the issuance of duplicate is not enough to carry out operations

bank accounts on behalf of the holders, certainly, to complete the scam, it is necessary to

It is necessary for a third party to “impersonate the identity” of the owner of the data before the entity financial. 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 any legal basis. guna, in addition to the violation of other principles such as confidentiality.

For this reason, this is a process in which the diligence provided by the operations doras is essential to avoid this type of scams and violations of the RGPD.

Diligence that translates into the establishment of adequate measures to guarantee Ensure that data processing is in accordance with the RGPD.

In short, the violation of the imputed administrative infraction responds to a precept included within "Principles related to treatment" that requires security adequate authority in the processing of personal data, security that has not been guaranteed according to the Proven Facts. And this is so, because it has facilitated do duplicate SIM cards to third parties other than the legitimate owners of mobile lines, after overcoming by these of the existing security policy tent, which shows a breach of the principle of confidentiality.

Illegality is the quality that has a behavior previously typical of vulnerability. generate the legal system and the purposes it pursues. In this way, to be sanctionable it is not enough that the conduct fits the description had in the type, but with it the objectives pursued are being violated by the law. In this regard, the conduct will be unlawful if the legal interest is damaged. protected by the precept violated.

In this case, the legislation on the protection of personal data pursues the fi- purpose that those responsible and in charge of the data carry out a treatment

of these having security measures that prevent illicit use or fraud.

slow of them. And this juridical right has been damaged in the objective facts.

of this procedure.

According to STC 246/1991 "(...) this different construction of the imputability of the autho-

The theory of the infringement of the legal person arises from the very nature of legal fiction.

ridiculous to which these subjects respond. The volitional element is lacking in them.

do strict, but not the ability to break the rules to which they are subjected.

Capacity for infringement and, therefore, direct blame that derives from the good ju-

protected by the rule that is violated and the need for such protection

is really effective and for the risk that, consequently, the person must assume

that is subject to compliance with said rule" (in this sense STS of

November 24, 2011, Rec 258/2009).

For these reasons, the claim is dismissed.

6. FIFTH ARGUMENT. – LACK OF PROPORTIONALITY OF THE PENALTY

PROPOSAL.

Regarding the breach of the principle of proportionality, the RGPD provides for ex-

specifically the possibility of graduation, through the provision of fines subject to

modulation, in response to a series of circumstances of each individual case.

dual. Although, this aspect will be analyzed in the Seventh FD.

ORANGE argues that the imposition of a fine for dissuasive purposes is not

justified in the present case, since it was not his will or intention

that these situations occur.

Of course, we do not doubt that the operator has the intention or will in

that these situations occur. But he confuses intentionality with negligence.

agency, this second being the determinant of the commission of the infraction.

The truth is that there has been an infringement of article 5.1.f) of the RGPD that should be sanctioned with a fine in view of the serious individual circumstances concurrent duals. Said fine must meet the characteristics imposed by the article 83.1 of the RGPD, that is, it must be individualized and effective, proportionate and deterrent.

The fine must be dissuasive, so that the offending conduct is not punished. tere in the future.

Let us remember that, regarding the imposition of a warning, reprimand, or the adoption of corrective measures in accordance with article 58 of the RGPD, a fine deterrent is one that has a genuine deterrent effect. In this regard, the Judgment of the CJEU, of June 13, 2013, Versalis Spa/Commission, C-511/11, ECLI:EU:C:2013:386, says:

"94. Regarding, firstly, 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)."

Furthermore, article 29.2 of the LRJSP also configures the function

discouraging or dissuasive of the fines by indicating that "The establishment of sanctions

pecuniary penalties shall provide that the commission of typified infractions shall not

is more beneficial to the offender than compliance with the rules violated.

you give".

The fine must generate a dissuasive effect regarding non-compliance and violation

tion of data protection regulations and never be more beneficial for

the offender than compliance with the rule violated.

On the other hand, ORANGE asserts that it must be considered to determine the amount

of the fine and its proportionality that has not obtained benefit, but has suffered

damage for the commission of the crime.

In addition to the fact that the production of possible damage to the person responsible for the treatment

protection is not considered a mitigating factor by protection regulations

of data and this is observed from the simple reading of articles 83.2 of the RGPD and 76.2

of the LOPDGDD, we remind again that the purpose of this procedure is

focuses on the absence of security guarantees that has allowed unauthorized access

authorized or illicit of third parties to the personal data of the interested parties.

The possible damages that it indicates that it suffers -attacks on its systems and assets- are

caused by its own negligence, since, if it had had measures

adequate security measures, such access by third parties would not have occurred and the crime

later would not have materialized.

Likewise, in his allegations he establishes as damages the fact of having had to carry out “in-

internal investigations, make compensation to the claimants and reevaluate pro-

procedures and protocols. All those damages related to internal investigations

and reassessment of procedures and protocols do not cease to be its own obligations

of the proactive responsibility that it imposes from risk management, among others

many duties, the maintenance, updating and control and auditing of the policies

data protection cases in an organization.

The compensations to the claimants also derive from the assignment of the damages

personal rights of those affected to third parties -enabling the subsequent commission of

crimes- which constitutes a fault also attributable to ORANGE, as a result of

the infringement of article 5.1.f) of the RGPD.

Likewise, the administrative fine will be effective because it will lead the company to

apply the technical and organizational measures that guarantee a degree of security

corresponding to the categorization of the type of transaction.

It is also proportional to the violation identified, in particular its seriousness,

the risks incurred and the financial situation of the company.

Likewise, the participation of ORANGE in the GT does not modify the responsibility that

now he is charged once the infraction is verified.

QUARTER. - PRINCIPLES RELATED TO TREATMENT.

It refers to the compensation received by the affected people from ORAN-

GE. In this regard, there is a communication addressed to claimant one, of

dated January 20, 2020, with the following tenor:

(...).

The measure adopted is considered to have the consideration of minimum essential

ble after the affected person lost the phone line.

He refers to the discarding of what he qualifies as "hypothetical assumptions" or "lucubrations" of

the Agency, not reported by any claimant: access to applications, use of re-

social des, etc. Well, these facts have not been considered as circumstances

individuals in the infringement charged to ORANGE, but rather offer a perspective

tive of possible risks derived from the treatment in question. risk management

It supposes an exercise of reflection that must be carried out before carrying out an activity.

treatment of personal data. Its objective is to identify and be able to anticipate

take into account the possible adverse effects, or unforeseen, that the treatment could have

about stakeholders. It must allow the person in charge to make the decisions and actions

necessary to ensure that the treatment meets the requirements of the RGPD and the

LOPDGDD, guaranteeing and being able to demonstrate the protection of the rights of the

interested.

Nor does the Agency confuse individual access to the SIM card with access to the

mobile terminal nor is it demanding any administrative responsibility in this regard.

Regarding the banking operations carried out and the security of the transactions

tions carried out by financial entities, it should be noted that these entities

are responsible for the treatment of their clients' data, and they are responsible for identi-

obligations than those indicated so far for the operators referred to the fulfillment

compliance with the RGPD and the LOPDGDD, and also those derived from the Royal Decree-law

19/2018, of November 23, on payment services and other urgent measures in matters

financial laugh.

It also invokes article 28.10 of the RGPD, well, from the beginning it must des-

letter that this precept allows the attribution of sanctioning responsibility to the

treatment manager. In the first place, because it clarifies that the provisions of the same

as it is “without prejudice to the provisions of articles 82, 83 and 84” (sanctioning regime

dor GDPR). And, above all, because the legal consequence provided for in article 28.10

It is not the sanctioning one, but the one of considering the person in charge as responsible for the treatment.

I lie. The conclusion is logical, since, if the former violates the Regulations “by de-

terminate the means and purposes of the treatment”, should be considered as responsible.

That is not what has happened in this file. In fact, it has not been proven

that actions have been carried out that entailed a "determination of the purposes and

means”, but, according to ORANGE itself, they would have failed to comply with any of the instructions issued by it in the customer identification processes.

Consequently, in no case is it appropriate to invoke article 28.10 RGPD for a presumed attribution of responsibility to those in charge, which, in addition, implies the exoneration of the controller (ORANGE as has been proven in this file).

ORANGE cannot avoid the responsibility that corresponds to the security treatment, hiding behind the breaches of those involved in the management tion of duplicate requests.

Regarding the two claims, we have previously clarified that this procedure procedure encompasses a broader investigation.

Regarding the fact that it has not provided data to third parties, the Security Office of the Internet user tells us that the “SIM card duplication or SIM card exchange - SIM Swapping-” “is based on the duplication of our SIM card, and for this, the at- cantes need some personal information, such as name and surname, DNI, date of birth, the last 4 digits of our bank account, etc., which have been able to obtain have by other means, such as phishing or buying from fraudulent online stores.

With this data, the attackers request a duplicate of our SIM, supplanting our identity with the above data before the operator. Meanwhile, the only thing What we notice is that our device runs out of mobile coverage, and when we connect we have a Wi-Fi network, we will begin to receive notifications of movements made two from our mobile without our consent, such as bank transfers or online shopping, among others.

An obligation of result is not required, but of activity, but in order to evaluate said tivity 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 process

of duplication, the safeguards implemented by ORANGE and inevitably, the re-

released.

Regarding the special relevance of the SIM card, we refer to the modern graduation

tivated in the Seventh FD.

Lastly, regarding the deployment of security measures, there is no doubt that

ORANGE has reviewed the protocols to prevent identity theft in

these processes; has transferred the information to those involved in the processing; has in-

introduced improvements after knowing certain vulnerabilities; including penalties

for its non-compliance. However, we do not share the fact that it has taken

carry out an appropriate and adequate deployment of security measures, in the terms

of article 32 of the RGPD.

It is not enough to have a security policy, but to adapt it to mitigate the

risks. The continuous advancement of technology and the evolution of treatments propitiate

cyan the continuous appearance of new risks that must be managed.

The risk approach and the flexible risk model imposed by the RGPD -based on

of the double configuration of security as a principle relating to the treatment and

an obligation for the person in charge or the person in charge of the treatment - does not impose in any

In any case, the infallibility of the measures, but their constant adaptation to a risk,

that, as in the case examined is true, probable and not negligible, high and with

a very significant impact on the rights and freedoms of citizens.

FIFTH. - SAFETY OF TREATMENT.

An infringement of article 32 of the RGPD is not imputed.

SIXTH. - GENERAL CONDITIONS FOR THE IMPOSITION OF THE ADMI-

NISTRATIVE.

Object of analysis in the Seventh FD of this Resolution.

SIXTH: Principles relating to treatment.

Considering the right to the protection of personal data as the right

natural persons to have their own data, it is necessary to determine the

principles that make it up.

In this sense, article 5 RGPD, referring to the "Principles related to treatment"

has:

1. The personal data will be:

a) processed in a lawful, loyal and transparent manner in relation to the interested party ("lawful

trust, loyalty and transparency»);

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 line with these provisions, recital 75 of the RGPD establishes:

serious and probable risks to the rights and freedoms of natural persons.

variable ity, may be due to the processing of data that could cause damage

and physical, material or immaterial damages, particularly in cases in which the

treatment may give rise to problems of discrimination, identity theft or

fraud, financial loss, reputational damage, loss of confidentiality of

data subject to professional secrecy, unauthorized reversal of pseudonymization or

any other significant economic or social damage; in the cases in which

sees the interested parties of their rights and freedoms or prevents them from exercising control over

about your personal data; in cases in which the personal data processed reveals

ethnic or racial origin, political opinions, religion or philosophical beliefs,

militancy in trade unions and the processing of genetic data, data related to health or

data on sexual life, or convictions and criminal offenses or security measures

related ity; in cases in which personal aspects are evaluated, in particular

the analysis or prediction of aspects related to performance at work, situation

financial, health, personal preferences or interests, reliability or behavior,

situation or movements, in order to create or use personal profiles; In the cases

in which the personal data of vulnerable persons, in particular children, are processed; either

in cases where the processing involves a large amount of personal data

and affect 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 two 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, their powers of disposal and control over their personal data are affected.

them, which constitute part of the content of the fundamental right to the protection of

data as indicated by the Constitutional Court in Judgment 292/2000, of 30

November 2000 (FJ 7). So, by getting a duplicate of the card

SIM, it is possible under certain circumstances, the access to the contacts or to the

applications and services that have as key recovery procedure the

sending an SMS with a code to be able to modify the passwords. Definitely,

may supplant the identity of those affected, being able to access and control, by

example: email accounts; bank accounts; apps like

WhatsApp; social networks, such as Facebook or Twitter, and much more. in short

accounts, once the password has been modified by the impersonators, they lose

control of your 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 after providing ORANGE duplicates of the SIM card to third parties.

people who are not the legitimate owners of the mobile lines and even modifying

enter the personal data -email or SIM number- (claimant party

one), after the supplanting people overcome the security policies

implemented by the operator, which shows a breach of the duty of protection

collect customer information.

This unauthorized access to the SIM card is decisive for the actions

developed by the supplanting people whose purpose is to obtain

have an economic benefit (there are up to five calls to Banco Santander and the

performance of ten banking operations in the case of the claimant one and one

operation, in the case of the complaining party two), since the impersonator takes advantage of the

period of time that elapses until the user detects the fault on the line,

contacts the operator, and this detects the problem, to carry out operations

fraudulent bank transactions after accessing the online banking passwords of the legitimate subscriber

I swim.

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

by which ORANGE have a legal duty to guarantee its safety, just as it would

with any other company 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

It reaches those public personal data that, 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 treatments

of personal data.

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

commission of the offence.

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

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

f) Affectation of the rights of minors.

g) Have, when not mandatory, a data protection delegate.

cough.

h) The submission by the person in charge or person in charge, voluntarily

to alternative conflict resolution mechanisms, in those su-

positions in which there are controversies between them 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:

 Nature and seriousness of the offence:

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 infringement is very serious

since it entails a loss of disposition and control over the data

personal. Allows criminals to steal identity through se-

after obtaining a duplicate of the number of the telephone number

your SIM card. After the entry into force of the PSD2 Directive, the telephone

mobile comes to have a very important role in making payments on-line

line as needed for transaction confirmation, and converts

to this device -and by extension to the SIM card-, with the clear objective of

cyber criminals.

Contrary to what ORANGE alleges, the seriousness of the infraction focuses

in the loss of disposal and control over the personal data of the

operator's customers due to the absence of appropriate security guarantees.

pious. The AEPD does not focus on previous or subsequent actions of

third parties, but rather in the actions or omissions of ORANGE that have

unauthorized or illicit access to the personal data of its clients is prohibited.

to third parties due to the absence of appropriate security guarantees,

matter that has been duly proven.

In all probability, if ORANGE had had measures of

appropriate security this transfer of personal data to third parties is not

would have produced

It is true that third parties have not accessed the mobile phones of

the interested parties, but yes to their personal data, as stated

manifest in this sanctioning procedure.

Likewise, it is not up to the AEPD to determine what the specifics are.
these security measures to be implemented, but to the controller
treatment, in-depth knowledge of its organization, treatments, vulnerability
nerabilities and the security measures required to make effective
vo the principle of integrity and confidentiality.

 Duration of the offence:

Although the facts denounced by the complaining parties occur
on certain dates, ORANGE declared in fiscal year 2019, (...) ca-
You are together with ORANGE VIRTUAL ESPAÑA, S.A.U (SIMYO).
ORANGE asserts that the infractions were punctual and quickly
solved and that the (...) cases are attributable to another legal company-
differentiated mind.

The sanctioning file has its origin in two claims
submitted to the Agency, although it has not only taken into account
the concrete facts and specificities that occurred in those cases, but
who has questioned the security measures adopted by ORANGE
in general. Thus, it must take into account all cases
of fraud declared by ORANGE itself together with ORANGE VIR-
TUAL ESPAÑA, S.A.U (SIMYO) that show a continuous evolution of
fraud cases.

In this particular, draw attention to the fact that together with the allegations to
the Proposal for a Resolution provides a Document 1 related to the
Complaint filed with the Superior Police Headquarters, Brigade
Provincial Judicial Police, Gº 7, of Madrid, by ORANGE ESPAÑA,
S.A.U. as harmed by the facts described in the complaint
(identity theft, fraudulent SIM card duplication and

bank fraud) of clients of ORANGE and SYMIO indistinctly,

when he states in his pleadings that they are two legal persons

different.

 Number of stakeholders affected:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

92/99

The Resolution collects the claims made by the two parties

claimants.

In addition, ORANGE reports a percentage of declared cases in the

financial year 2019 (...) with respect to the total number of clients (...) reached

a (…) %.

Reports on the completion of approximately (...) SIM changes,

cases of fraud reaching a (...) % of the total changes of card-

SIM cards made.

Given that, as has been explained, the object of the sanctioning procedure

The claimant is not limited to the two claims presented, but

the absence of security guarantees and unauthorized or illegal access

I quote from the data, it is considered the overall figure referred to.

 Level of damages suffered:

Tall.

It argues that practically all the operations have not given rise to

no contingency, nor has there been any damage or loss and that

carrying out banking operations is completely unrelated to duplication.

cation of the SIM card.

However, the proven facts show that after the issuance of the

duplicates, fraudulent banking operations have been carried out that

They happen in a short space of time. By duplicating the

SIM cards, would-be impersonators gain control of the line

line of the subscriber and specifically the reception of SMS addressed to the legitimate

subscribed to carry out on-line operations with banking entities

Planting your personality.

ORANGE is not responsible for customer identification policies.

established by banking entities. However, it is also

true, that if ORANGE ensured the identification procedure and

delivery of the duplicate SIM card, the system could not even be activated.

issue of verification of banking entities. the scammer person

after getting the activation of the new SIM, take control of the line

phone, thus being able, then, to carry out banking operations

fraudulent accessing the SMS that the banking entities send

to their clients as confirmation of the operations they execute. Is

sequence of events revealed in the international claims

put in place generates a series of serious damages that should be

be taken into account in an impact assessment relating to the pro-

data protection (considering 89, 90, 91 and article 35 of the RGPD). In

definitively, from the moment a duplicate is delivered to a person

other than the owner of the line or authorized person, the customer loses the

control of the line and the risks, damages, multiply. Ade-

Moreover, the events occur with an overwhelming immediacy.

Regarding the allegations made by ORANGE regarding the fact that

It is not possible to attribute the damages to ORANGE or consider them

as aggravating factors, we must furthermore mean that it is a

damage itself unauthorized or illicit access to personal data

of an interested party by a third party when violating the Fundamental Right

as to the protection of personal data.

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:

He argues that his conduct must be considered diligent and act this

made as a mitigation of the sanction.

Although the Agency considers that there was no intent on the part of

ORANGE, the Agency concludes that it was negligent in failing to secure a

procedure that guarantees the protection of the personal data of

Your clients. Thus, a socially harmful result is produced.

ignoble that imposes the disapproval of the security policy implemented

gives.

Deny the concurrence of a negligent action on the part of ORAN-

GE would be equivalent to acknowledging that its conduct -by action or omission- has

been diligent. Obviously, we do not share this perspective of the

chos, since the lack of due diligence has been proven.

A large company that processes the personal data of its

customers on a large scale, systematically and continuously, must take extreme

care in fulfilling its obligations in terms of protection

tion of data, as established by jurisprudence. It is very illus-

tive, the SAN of October 17, 2007 (rec. 63/2006), based on

that these are entities whose activity is accompanied by continuous

processing of customer data, indicates that "…the Supreme Court has

ne understanding that there is recklessness whenever a

legal duty of care, that is, when the offender does not behave with

the due diligence. And in assessing the degree of diligence,

weighing especially the professionalism or not of the subject, and there is no

doubt that, in the case now examined, when the activity of the

current is of constant and abundant handling of data of a personal nature.

sonal

must insist on rigor and exquisite care to adjust to

legal provisions in this regard.

Also, contrary to ORANGE's assertions, when the

AEPD indicates that the operator "was negligent in not ensuring a pro-

procedure that guarantees the protection of the personal data of its

customers", does not impose strict liability regarding the measures

give security This is so, because this statement must be put into

its context: in a violation of the principle of confidentiality as

as a result of negligence in implementing the measures

appropriate to which article 5.1.f) of the RGPD refers to to earn

guarantee that confidentiality. It is undeniable that unauthorized access

or illicit of the personal data of the affected party has been produced, derived,

in this case due to a lack of adequate security measures.

- Article 83.2.d) RGPD:

 Degree of responsibility of the person in charge:

Tall.

Responsibility for vulnerabilities in the implanted procedure

ted for the issuance of the SIM corresponds to ORANGE. The charge-

parties to the processing -if applicable- can only process the following data:

following the documented instructions of the person in charge.

The personal data that ORANGE collects both for contracting

of the service as during its provision are your responsibility and de-

must be treated in a way that allows the good development of the relationship

contractual agreement between the parties, guaranteeing at all times the application

cation of the principles of article 5 RGPD. And this is independent of

that the treatment is carried out by itself or through a person in charge of

treatment.

In this sense, article 28.3.h) of the RGPD establishes instruments of

continuous supervision by the person in charge of the treatment when indicating

that the person in charge “will make available to the person in charge all the information

information necessary to demonstrate compliance with the obligations

established in this article, as well as to allow and contribute

to the performance of audits, including inspections, by the

person in charge or of another auditor authorized by said person in charge”.

Regarding the performance of audits as an ideal means for

the data controller continuously supervises the processor

of treatment, CEPD Guidelines 07/2020 establish that:

“99. The obligation to use only data processors

"that provide sufficient guarantees" contained in article 28,

section 1 of the GDPR is a continuous obligation. It doesn't end in the mo-

moment in which the controller and the person in charge of the treatment celebrate a

contract or other legal act. Instead, the controller must, at intervals

appropriate, verify the guarantees of the processor, including through autho-

reports and inspections when appropriate". (The translation is ours).

Article 83.2.e) GDPR:

-

 Any previous infringement committed by the data controller:

It should be noted that recital 148 of the RGPD adds that it must

refer to “any previous relevant” or “relevant” infringement of the

translation of the original text in English “relevant”.

For this reason, we only consider a procedure in which a sanction has been

ORANGE (firm administrative decision) as a result

consequence of the treatments carried out without legitimation resulting from

an identity fraud.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

95/99

Infraction imputed

gives

Sanction

6.1 GDPR

80,000.00

Procedure No.

I lie

PS/00452/2019

Resolution date

sanctioned

dora

06/23/2020

- Article 83.2.g) RGPD:

 Categories of personal data affected by the breach:

ORANGE argues that only basic data of the

customers and that the SIM card is not personal data, since

we beat this argument in the FD Fourth.

The Agency considers unauthorized access to a duplicate card

SIM is considered particularly serious as it enables spoofing

of identity. Hence, we consider the stolen data as

sensitive nature.

The delivery of a duplicate SIM in favor of a third party other than the lender

legitimate owner is considered particularly serious since it makes it impossible to

sending or receiving calls, SMS, or access to data service,

which happens to be in the hands of the supplanting person.

Obtained the duplicate, the path to the applications and ser-

vices that have as a key recovery procedure the en-

sending an SMS with a code to be able to change the passwords. In

In addition, it enables identity theft.

It is not about the personal data that is required for the issuance of the du-

plicate of the card, but of the card itself as personal data associated

ciated to a telephone line owned by 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 perform operations on their behalf, authenticating themselves

by a username and password previously taken from that user,

as well as with double-factor authentication when receiving the confirmation SMS.

signature on your own mobile terminal where you will have inserted the card

Duplicate SIM.

In this sense, bringing up again the aforementioned SAP of Barcelo-

na no. 390/2019 of May 30.

~

Article 76.2.b) LOPDGDD:

 Linking the activity of the offender with the performance of treatment

personal data:

The development of the business activity carried out by ORANGE re-

wants continuous and large-scale processing of personal data

of customers, according to the number of mobile voice telephone lines

formed in the "EIGHTH Antecedent", which positions ORANGE

as one of the three largest telecommunications operators

of our country.

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

suffered by the interested parties:

positive. Namely:

(...).

It also provides for compensation for damages suffered.

- Article 83.2.f) RGPD:

 Degree of cooperation with the supervisory authority:

Tall.

The Agency considers that ORANGE has cooperated favorably

with the investigation, providing response to the requirements and

forming part of the GT, which is valued positively.

- Article 76.2.c) LOPDGDD:

 The benefits obtained as a result of the commission of the investment

fraction.

This Agency does not consider that ORANGE has obtained a benefit

beyond receiving the cost price set for the issue

of duplicate SIM cards.

- Article 76.2.h) LOPDGDD:

 Submission to conflict resolution mechanisms.

Various telecommunications operators, including

ORANGE, signed a Protocol with AUTOCONTROL that, without per-

judgment of the powers of the AEPD, provides mechanisms for

the private resolution of controversies related to data protection

in the field of contracting and advertising of communication services

electronic forms, dated September 15, 2017. Protocol whose

effective enforcement should be considered mitigating.

The following extenuating circumstance must be taken into account:

- Article 83.2. j) GDPR:

Regarding adherence to approved certification mechanisms

under article 42.

ORANGE has the Certificate of conformity with the National Scheme

tional Security.

The allegations made in relation to article 83.2.a) are rejected.

b), d) and g) of the GDPR in the terms set forth above.

Likewise, the one set forth in article

76.2.a) of the LOPDGDD, regarding the continuous nature of the infraction,

because the lack of concurrence of the budget for its application entails

that cannot be taken into consideration, following the criteria expressed

by the SAN, Contentious-administrative Chamber, Section 1, of May 5

2021, Rec. 1437/2020, which says: “Considers, on the other hand, that it must learn

The non-commission of a previous infraction may be cited as a mitigating circumstance. As 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 infringement previous fraction committed by the person in charge or the person in charge of the treatment to". This is an aggravating circumstance, the fact that he does not attend the budget for its application implies that it cannot be taken into consideration, but does not imply or allow, as the plaintiff claims, its application cation as a mitigating factor”.

Finally, ORANGE requests that the fine be replaced by "the adoption of the measures corrective measures contemplated in the aforementioned article 58, consisting of the warning or warning to the controller and the imposition of the obligation to adopt tion of measures to carry out the treatments “in a certain way and within of a specified period”.

This request must also be dismissed. Understanding the corrective system provided for in the RGPD that ORANGE proposes is wrong.

Article 83.2 of the RGPD provides that "Administrative fines will be imposed, in depending on the circumstances of each individual case, in addition to or as a substitute for the measures contemplated in article 58, section 2, letters a) to h) and j)”.

The same provision is included in article 58.2 of the RGPD regarding the powers corrective actions of the control authorities, in which section i) provides: "impose a

administrative fine under article 83, in addition to or instead of the measures

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

lar".

In the same sense, recital 148 of the RGPD states that: "In order to reinforce the

application of the rules of this Regulation, any infringement of this must be

be punished with sanctions, including administrative fines, in addition to

appropriate measures imposed by the supervisory authority under this Regulation.

regulation, or in substitution of these".

This means that the administrative fines are imposed additionally, that is, they are

imposes a fine in addition to one of the corrective measures provided for in article

58.2. letters a) to h) and j) of the GDPR. Or, that the administrative fines are imposed by way of

substitute for the aforementioned corrective measures, that is, a substitute fine is imposed.

going to one or several of those measures. Thus, the fine is not replaced by one of the

corrective measures, if any, but rather the opposite.

Furthermore, recital 148 of the RGPD provides that: "In the event of infringement

minor, or if the fine likely to be imposed constituted an undue charge.

provided for a natural person, instead of a sanction by means of a fine,

put on a warning". This provision entails the necessary imposition of a

fine in any case, in addition to other corrective measures that may additionally be

establish, if the infringement is considered serious for the purposes of the Regulation in

attention to the circumstances established in the aforementioned recital and in article 83 of the

GDPR.

Therefore, in accordance with the applicable legislation and after assessing the graduation criteria

tion of the sanctions whose existence has been proven, the director of the AEPD

RESOLVES:

FIRST: IMPOSE ORANGE ESPAGNE, S.A.U., with NIF A82009812, for a

infringement of article 5.1.f) of the RGPD, typified in article 83.5.a) of the RGPD and quali-

classified as very serious for prescription purposes in article 72.1.a) of the LO-

PDGDD, an administrative fine amounting to 700,000'00 euros (seven hundred thousand

euros).

SECOND: NOTIFY this resolution to ORANGE ESPAGNE, 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 Spanish Agency for Data Protection within one month from tar from the day following the notification of this resolution or appeal directly contentious-administrative before the Contentious-administrative Chamber of the Audien- National Authority, in accordance with the provisions of article 25 and section 5 of the Fourth additional section of Law 29/1998, of July 13, regulating the Jurisdiction Contentious-administrative, within two months from the day after to the notification of this act, as provided in 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

938-26102021

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es