 File No.: PS/00046/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

BACKGROUND

FIRST: A.A.A. (hereinafter, the claimant party one), on September 2 2019, files a claim with the AEPD against ORANGE ESPAÑA VIRTUAL, S.L. with NIF B85057974 (hereinafter, SIMYO), for the following reasons:

“On 8/14/19 my mobile phone owned by me with number ***TELEFONO.1 belonging to the SIMYO operator, it does not have a line, so the area consulted staff of said operator from my computer, in the menu section it reads verbatim:

SIM change Mission accomplished! We have already delivered your duplicate SIM, remember that to activate it you have to go to the section DUPLICATE / ACTIVATE SIM from the menu.

DATE OF REALIZATION DATE 08/14/2019 TIME 21:15:40 TELEPHONE NUMBER ***TELEPHONE 1.

When reviewing the personal data recorded in the SIMYO application, it is observed as the email account has been changed, deleting the one from which subscribes, and consigning the account ***EMAIL.1 not knowing the reason for this change.

At this time proceed to change the keys of the SIMYO application to avoid a new fraudulent access, and to suspend the three (3) contracts of postpaid, which I have with said company, passing the numbers ***TELEFONO.1, ***PHONE.2 and ***PHONE.3 to the OFF status, no

being able to make or receive phone calls.

This party wishes to state that it has not applied to the SIMYO company for any

duplicate SIM card, so it is proven that my phone

particular ***TELEFONO.1 has been kidnapped and criminals have accessed

the application of the bank ING DIRECT in a fraudulent way through the control of the

mobile phone number.

Contacted the SIMYO operator, they report that said request for

DUPLICATE SIM card has been made in a physical store, and has been

purchased a duplicate SIM.

Asked in which store such manifest duplicate purchase occurred

that this information would be made available to the Authorities

police/judicial when they know that the incident has been reported

legally. This party has denounced everything that happened before the Judicial Police of the

Huelva Civil Guard, complaint No. XXX/XX. The Civil Guard has reported that the

Fraudulent duplication of the SIM card has occurred in a store in Barcelona

and that the employee who did it is identified as reported by ORANGE. Is

The party can submit the complaint to the Judicial Police if they require it opportunely.

SIMYO has violated my personal data and with it has proceeded to create

of a fraudulent duplicate SIM card which has served to do in the name

which signs two transfers of ten euros (sic) a payroll account and the

creation of a fraudulent personal loan of 43,000 euros. all because

SIMYO did not keep or have a duty to take care of my personal data.

I request that the AEPD sanction SIMYO in an exemplary manner.

I have addressed SIMYO through the channels they have established and they do not answer.

Call 121 FREE from your SIMYO mobile. (Hours: Monday to Sunday, from 8:00 a.m. to

23:00 hrs.) If you cannot call from your SIMYO mobile, call free to 1644

from any landline or mobile. in the email support@SIMYO.es I have addressed them and

they give me silence."

Along with the claim, it provides the complaint filed with the Organic Unit of the

Judicial Police of the Civil Guard, Huelva Command, on August 15,

2019, with number of proceedings XXX/XX, in which it states:

"(…) exposes some events that occurred on August 14, 2019, consisting of

having suffered an identity theft, which as a consequence, has

replaced both on the mobile phone line, taking out a duplicate of the card

SIM of the number ***TELEFONO.1, line this registered in ING for the

online operations, such as access to your bank account of the ING entity, therefore

that by modifying your keys, you can no longer have access to it, with the

consequent economic damage that derives (...)

It is tried by this part with great nervousness and late at night, to enter the

ING DIRECT application to check the balance of the accounts and I cannot access

yield, being blocked to the introduction of three times, since the keys do not

They worked, showing that they have changed my access codes.

Next my wife tries to access B.B.B., since she is a co-owner of the

bank accounts and she can access it, noting that it exists in the positions

a fraudulent personal loan amounting to 43,000 euros, the amount of which eco-

nomic was deposited in the orange account of which I am the holder.

Likewise, there is a bank transfer made from my account ***ACCOUNT-

TA.1 (ING) for an amount of 10,000 euros to the account ***ACCOUNT.2 (BBVA).

At 9:35 p.m. on August 14, 2019, the undersigned receives in his email

private email from Gmail, from the ING DIRECT bank, where it reads, “DOCUMEN-

ORANGE LOAN TATION”, “Dear A.A.A., thank you for choosing us for the

contracting your loan (...)

At 9:43 p.m. on August 14, 2019 (…) you receive in your email

(…) an email from the ING DIRECT bank, which reads, “Dear Mr. A.A.A., (…)

We attach a copy of the documentation related to your contract (...) product

contracted payroll account number ***ACCOUNT.3, where the

all personal data of this part (…)

To state that with my telephone number ***TELEFONO.1, after reviewing

Outgoing and incoming calls from the SIMYO operator application, are

make a phone call to the number 912518375 at 22:36:22 on 8-14-2019, yes

well the one who subscribes, does not make the call and they pretend to be me. said number

(...) corresponds to the BBVA Customer Service, for which the offenders

tell, they make that call to change the passwords of the bank (...)

It is requested that this case be audited as soon as possible by the services of

ity and security of the banking entity ING DIRECT, so that it is canceled and left

without effect both the orange loan number ***PRÉSTAMO.1 for the amount of

43,000 euros opened fraudulently and the account number ***ACCOUNT.3,

since both products have not been contracted by this party and have obvious

samples of banking fraud through the internet. “

Said complaint was subject to extension, on August 21, 2019, in which

states:

“(…) That the creation in the positions of the undersigned of the entity

bank ING, of three financial cards which are of fraudulent creation and

They are cancelled, but they are reported for the record and could have effects:

Debit card in the name of A.A.A. ***CARD.1

Debit card in the name of A.A.A. ***CARD.2

Credit Card in the name of A.A.A. ***CARD.3”

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 November 11, 2019, the claim was transferred to SIM-

ME, to proceed with its analysis and give an answer within a month.

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

following:

“ (…) On August 14, 2019, it was verified that, (…) “SIM change/duplicate” to

9:15:40 p.m.

(...) to the new value ***EMAIL.1 by (...) at 18:55:30, (...) “change/duplicate

of SIM”.

The next day, August 15, 2019, Mr. A.A.A. gets in touch with

SIMYO, through the Customer Service (Call Center) indicating that it does not

recognizes neither the duplication of the SIM card made, nor the modification of

contact details (email) made. Given this story, transfer

of what happened to the Fraud Department, so that it analyzes in depth what

happened, while, in parallel, it is verified that both the change of

SIM card like the rest of the lines whose ownership corresponded to D.A.A.A.,

had been voluntarily suspended by the client, an operation that had

processed through your Personal Area.

On August 16, after the corresponding analysis of the facts, the

contacting the customer and after offering a duplicate SIM before placing the order

of definitive discharge, which is rejected, is carried out, at the request of Mr. A.A.A., the

deactivation of all your lines contracted with SIMYO. (...)

(...) As we have had the opportunity to highlight in the letter of

response to information request E-08994-2019, notified last

November, (...), the Orange Group in Spain, of which it is also a part

SIMYO has reinforced and strengthened the Protocols implemented for the processing

of certain acts (among which are the duplication of cards

SIM).

Indeed, it is stated that, having detected that the operation

used by alleged phishers in the SIMYO brand

consisted of (...), new modifications have been implemented in the procedure

established, in order to provide it with additional measures for greater robustness.

First of all, SIMYO has eliminated the possibility of (…), dated August 23

of 2019, in such a way that (...). This measure has been adopted bearing in mind

the nature of SIMYO Points of Sale, since they are not stores

own.

Secondly, and in relation to the above, the measure has also been adopted

of (…), because although until the date August 26, 2019 it was possible (…)".

Thirdly, and bearing in mind that currently both the sending of the card

SIM as the subsequent activation is only possible by (...), SIMYO has

implemented, on August 26, 2019, various additional measures in the

performance of certain acts, with the aim of guaranteeing the identity of the

client in order to avoid the repetition of situations similar to the one we

occupies.(…)"

On said claim fell resolution of ADMISSION TO PROCESS dated 18 of

December 2019, in the file with no. of reference E/10534/2019.

SECOND: C.C.C., (hereinafter, the claimant party two), on November 6

of 2019, file a claim with the Granja de Torreher Post Office.

mosa, which is registered with the AEPD on November 13, 2019, addressed

against SIMYO, for the following reasons:

"(…) as of August 23, 2019, SIMYO being my telephone company,

communicates urgently to the same (via telephone and electronically) that

someone has wanted to obtain personal data on behalf of SIMYO.

A superior of SIMYO (D.D.D.) exposes me who has been brought to the attention of

the whole team what happened so that no modification or change is made in

the affected line (***PHONE.4).

An hour later, the affected person loses coverage on the phone at

consequence of someone from the SIMYO company having made a duplicate of

SIM card without the consent of the owner of the line.

The affected person calls the company from another terminal, reporting that he does not have

coverage on your phone. At this time, the same person who attended you

above, tells you not to worry, that everything is in their hands, that

in 3 days they will solve it and that they will compensate you for what happened; not commenting on

no time that a duplicate SIM card had been made.

This fact entails a series of damages and losses to the affected party and his family, since

by duplicating your SIM, outsiders obtained all kinds of data, including

banks, using them to carry out a subtraction of (30,000 Euros) from

the bank account shared by the affected person with his family, who had to

block all bank accounts and credit cards, in addition to suffering

psychologically by this fact, affecting their health.

On the other hand, the affected party had to request vacation days from his job to

carry out the relevant banking procedures. Secondarily, but no less

importantly, the affected party has been held incommunicado indefinitely and without

be able to unsubscribe said line, when the authors of such act modify their data

bill. (…)"

Along with the claim, it provides the complaint filed with Post P. de Rincón de

la Victoria, of the Malaga Civil Guard Command, on August 24

of 2019, with report number *** COMPLAINT.1, in which it states

"(…) STATES that he is the holder of a bank account in the entity Banco

Santander with account number ***ACCOUNT.4, in which it appears as persons

authorized the father of the complainant D. E.E.E., his mother Dª F.F.F. and the brother

of the complainant D.G.G.G..

That on August 23, 2019, at approximately 10:45 p.m., the complainant

accesses the Banco Santander account inquiry application, and

you can check how the amount of 30,000-- euros has been withdrawn from the account,

who immediately makes a phone call to his parents to find out the reason

of said withdrawal, and that his parents inform him that they have not made any

movement of that amount.

That he immediately makes a call to the bank, to the telephone number

900.811.381, in which the operator informs him that if he had accepted any

email of the Santander bank entity, being informed the operator

by the complainant, that he has not accepted any email and that he has not

provided any data to any person, nor has it lost any type of

documentation.

That in this call the access to multichannel was blocked, and by application to the

bank account, as well as digital signatures.

That the complainant is informed by the operator of the entity that his parents

they should cancel, the bank account, as well as cards of said entity,

procedures that his father carried out on August 24, 2019 around 00:30 hours, since

that although the owner is the complainant, he was very nervous to

carry out this type of procedure, due to having doubts that he may have been the victim of a

Crime of fraud.

That the complainant receives a call on his mobile terminal with a number

***TELEFONO.4, which operates with the company SYMIO, with a hidden number and

privately, around 1:35 p.m. approximately, in which a

male interlocutor, several questions without being related to the

complainant, such as providing their ID, date of birth, etc., that the interlocutor

he had a Spanish accent, apparently from the north of Spain.

That the complainant receives a second call with a hidden and private number in the

aforementioned terminal, at 4:12 p.m., on August 23, 2019, in which the

male interlocutor, says: Hello, I'm calling you from SIMYO, (offering you an offer of

data and calls), asking the complainant for their date of birth, providing

the interlocutor his date, the interlocutor informing the complainant that if he wanted

verify the offer by calling the number 1644, the customer service number of the

SIMYO company.

That the complainant makes a call to 1644 to verify the veracity of the

offer and is informed that the company has not offered him anything.

That the complainant sends an email to the aforementioned company to notify

from what has occured.

That the complainant checks how his mobile terminal is left without coverage,

contacting the SIMYO company again to find out the reason for this

incidence, being informed by the company, that it did not have coverage due to issues of

security, and that on Monday the problem would be resolved.

That through the personal area (...), you can see a message, at 04:57 hours

day 08-24-2019, in which it is stated that there has been a duplicate of the card

SIM, which occurred at 5:48 p.m. on 08-23-2019, being of special

interest since this duplication takes place approximately one hour, that the

complainant inform the company of the calls received with a hidden number

and private.

ASKED to say or provide the data available from the extraction

of the amount of 30,000 euros.

STATES that it has occurred through bank transfer, which has not

been authorized by the complainant, nor has it proceeded to enter codes of

confirmation, nor make the electronic signature, not knowing how it has been possible

produce said transfer, that the account where the money has been transferred is the

next ***ACCOUNT.5 where Hhh (sic) appears as beneficiary, you cannot

provide an extract of the movement, because the entity is closed due to being a weekend,

and not being able to access your checking account through the entity's application

for having the mobile phone blocked.

That the amount transferred is 30,000 euros. (…)"

Likewise, it provides the message dated August 23, 2019, in which SIMYO informs

who has already delivered the duplicate SIM, as well as the email that the party claims-

you two addressed to support@simyo.es, on that same date, informing about the reception

of a call with a hidden number pretending to be SIMYO.

On January 9, 2020, the claim was transferred to SIMYO, so that

proceed to its analysis and respond within a month.

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

following:

"(…) On August 23, 2019, it is identified (…), corresponding to the

request for a duplicate SIM card corresponding to the numbering

***TELEPHONE.4 from (…).

(…)".

Taking into account the foregoing, it has been confirmed that (…).

As has been verified, after identifying repeated attempts to obtain

access to the claimant's personal area, this company proceeded to (...) Mr.

C.C.C.. It is worth noting that, as has been shown throughout the

present, as soon as this merchant became aware of the indications that

They warned of an irregular treatment of the data of Mr. C.C.C. on the occasion of

duplicate of the SIM card numbering ***TELEFONO.4, proceeded (...).

After the above, in the month of October 2019, it was received in the systems of this

mercantile official claim in relation to the facts warned and that bring cause

of this requirement. After a study of the case, and out of commercial deference,

this mercantile (...).

Given the foregoing, being SIMYO (...), this company focuses all its

efforts in the constant implementation of security measures and

authentication, which allow guaranteeing the true and secure identification of the holder in

In order to combat this type of fraudulent process, as we will explain later

ahead.

Due to the above, Orange has proceeded to send it through a communication

sent by burofax, a copy of which we attach to this letter as

attached document No. 1, through which we have proceeded to inform the

claimant of the measures carried out by this company on the occasion of the

this request, as well as the actions described in this report.

(...) It should be noted that there is a (...) in relation to an alleged SIM duplicate

not consented to any of its brands.

Well, in saying (...). We provide the procedure as attached document No. 2.

For its part, SIMYO has eliminated the possibility of (...), in such a way that, from

that date, it is no longer possible to purchase the SIM card in a (...). Similarly,

The measure of (...) has also been adopted.

On the other hand, and bearing in mind that currently so much (...), SIMYO has

implemented, on August 26, 2019, various additional measures in the

performance of certain acts, with the aim of guaranteeing the identity of the

client in order to avoid the repetition of situations similar to the one we

occupies.

Likewise, it is of interest to show the Agency to which we have the honor to

we direct, there is a (...) to achieve technological developments and improvements

necessary for the requests of (...).

This new technology would allow, (...)".

On said claim fell resolution of ADMISSION TO PROCESS dated 13 of

November 2020, in the file with no. of reference E/00220/2020.

THIRD

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

news appeared in the media regarding the use of practices

fraudulent based on the generation of duplicate SIM cards without the

consent of their legitimate owners in order to access information

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

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

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

existing security measures for its prevention.

Namely:

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

| Economy | THE COUNTRY (elpais.com)

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

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

bank | Technology (elmundo.es)

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

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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 requests addressed to SIMYO, on different dates:

Secure Verification Code Requirement

First

Second

Third

***CSV.1

***CSV.2

***CSV.3

Required date

I lie

Notification date-

tion required

I lie

01/13/2020

06/24/2020

09/16/2020

01/13/2020

06/25/2020

09/17/2020

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

Next information:

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

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

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

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

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

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

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

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

he saw.

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

their attention. Documentation proving its dissemination among the companies

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

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

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

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

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

method used.

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

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

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

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

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

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

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

procedure to improve security.

7. Number of cases of fraudulent duplicate SIM requests detected

two throughout the year 2019.

Total number of mobile telephony clients of the entity.

In the second of the requirements, dated June 24, 2020, the

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

SIM), where the data 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.

B). 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.

C) In home deliveries, information is requested on whether it is possible to change the

SIM delivery address and under what circumstances and controls.

D). 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. The list will include SIM duplicates

requested since January 1, 2020, that is, all those claimed that

yielded from January 1, from the first, consecutive until reaching

twenty.

It is requested to indicate in the list only:

- the date of the SIM change,

- the line number,

- request channel,

- delivery channel.

POINT 3

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

10/88

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) In both cases, it appears that the request was made at a point of sale (the

made before 08/26/2019).

The reason why the SIM duplication was possible in these previous cases is requested.

essential. Documentary accreditation of the controls that were passed on the

identity of the applicant in stores.

B) In both cases the email address was previously changed

to the request.

Information is requested on how the email addresses of the clients changed

and documentary accreditation of the controls that were passed for the identification

of the client in each case.

C) Channels through which activation occurred. Documentary accreditation of the

controls that were passed on the identity at activation, in each case.

D) In case E/00220/2020, the client mentions that he alerted the entity

prior to the alleged identity theft of a possible attempt to use fraudulent

dulent of your data.

Information is requested on the reason why it was not marked or taken into account

such information to prevent identity theft to issue duplicates

of SIM.

E) 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 prevent possible attempts

of future identity theft.

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

point of sale.

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

lares.

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

resolution of your case.

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

requested the following information:

POINT 1

Regarding the list of 2 cases of SIM duplicates denounced/claimed facilitated

mentioned in the previous answer:

It is requested, in the first case, in relation to the duplicate SIM that was reached

change:

A. Copy of the DNI or identification documents provided by the applicant in the

point of sale.

B. About activation by the Call Center:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

11/88

- copy of the recording of the conversation where the applicant exceeds the policy

of security.

It is requested, for the change attempts requested in both cases:

C. Detailed information on how canceled and circulated attempts were detected.

circumstances for which they were classified as fraud or unrealizable. Policies or

controls that did not pass such requests.

D. Information on the reasons why a change of

SIM in the first case, having been 2 previous attempts. information about whether

first fraud attempts were classified and controls put in place to

ensure possible successive attempts.

FIFTH: On January 28 and July 1, 2020, SIMYO requests 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 deadline for a period of five days.

SIXTH: In response to the three requests made, SIMYO provided the following

information that was analyzed by this Agency:

1.- Information on the routes available to customers:

(…)

2.- Detailed information on the procedure:

(…)

SIMYO representatives have stated that:

(…)

The security policy explicitly consists of:

(…)

C) Information has been requested on whether it is possible to change the shipping address

SIM delivery and under what circumstances and controls.

In the aforementioned document “(…)” it is established that:

(…)

On the change of the client's address in the entity's systems, the re-

SIMYO representatives have stated that currently there are only two

possibilities:

(…)

It is stated in the document that:

(…)

D) About the checks that are carried out in the home delivery of the tar-

SIM card for recipient identification.

(…)

On the number of cases of fraudulent requests for SIM duplicates de-

detected throughout the year 2019, the entity has stated:

In relation to the ORANGE group, that: “The number of cases detected during

in 2019 it amounted to ***NUMBER.1 assumptions. This figure, compared to the number

total customers in 2019 (16,312,653), represents a ***NUMBER.2%.

Approximately ***NUMBER.3 SIM changes are made annually.

The cases of fraud detected, currently and despite the efforts made

two, represent a ***NUMBER.4% of the total SIM card changes made.

zeds."

Regarding the cases presented to the agency:

CLAIMANT PARTY ONE:

- SIM change request: (...)

A copy of the DNI or identification documentation has been required, as well as the rest

of associated documentation, provided by the applicant in (...). It is not provided.

(Note that it is done before 08/26/2019 when SIMYO changes its (...)).

The representatives of the entity indicate that the impersonators acquired the

SIM cards in (...) which shows that said (...) must have provided them (...).

Indicate that (…). It is currently disabled.

SIMYO's representatives state that (...). They point out that they

knew certain identifying data of the client.

- Damages: Fraudulent banking operations are reported using the

SIM copy.

- Actions taken. The representatives of the entity indicate that:

o SIMYO has strengthened its Security Policy by reinforcing the Protocols

existing ones (...) such as, for example, (...), which, as we have said,

is currently disabled.

either (…)

They also indicate that operational changes have been made so that these following

situations do not take place again in the future, among which we can mention the

following:

(…)

CLAIMANT PARTY TWO:

- SIM change request: (...).

A copy of the DNI or identification documentation has been required, as well as the rest

of associated documentation, provided by the applicant at the point of sale.

It is not provided. (Note that it is done before 08/26/2019 when SIMYO changed

bia his (...)).

The representatives of the entity indicate that the impersonators acquired the

SIM cards in (...) which shows that said (...) must have provided them (...).

They indicate that (...), because at that time, this functionality still existed in

the same. It is currently disabled.

The representatives of the entity have stated that:

(…)

- Damages: Fraudulent banking operations are reported using the

SIM copy.

- Controls: Since the client mentions that he alerted the entity, so

prior to the alleged identity theft, of a possible attempt to use

fraudulent use of your data, SIMYO has been asked for information about and the

reason why such information was not marked or taken into account for

prevent identity theft to issue duplicate SIMs.

SIMYO's representatives have stated in this regard that the facts

are summarized as follows:

(…)

- Actions taken: They provide the same allegations as in the case of

the complaining party one.

On other cases not filed with the agency:

The representatives of the entity have stated in this regard that only

nest knowledge of ***NUMBER.5:

(…)

Specifically, the complete process of the case was as follows:

On 03/26/2020 an attempt is made (…)

On 03/27/2020 they meet (...)

On 03/28/2020 an attempt is made (...)

On 03/28/2020 the SIM activation of the 26th is attempted (...)

On 04/01/2020 it is purchased (...). Activation of this occurred.

They provide a copy of the recording where the security policy is exceeded if

well indicate that this security policy has been strengthened since then.

stop

Listening to the recording, the operator requests (...)

SIMYO indicate that it has modified the established procedure, demanding

that (…)

In this case, therefore, (...)

The representatives of the entity state that it was possible to avoid duplication

of the SIM (...)

SEVENTH: On February 3, 2021, commercial information is obtained on the

SIMYO's sales volume during the year 2019, being the results of

123,577,000.00 euros. The share capital amounts to 9,535,587.00 euros.

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

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

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

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

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

72.1.a) of the LOPDGDD, and may be sanctioned with an administrative fine of

100,000.00 euros (one hundred thousand euros), without prejudice to what may result from the instruction.

NINTH: On February 12, 2021, the AEPD, in compliance with the provisions

in article 77.2 of the RGPD communicates to the complaining parties one and two, the in-

coercion of sanctioning file PS/00046/2021.

TENTH: The Initiation Agreement is notified to SIMYO, on February 15,

2021, through Citizen Folder, according to confirmation of receipt that appears

on the record.

ELEVEN On February 16, 2021, SIMYO files a document through the

which requests the extension of the term to submit allegations and provide documents or

other judgment elements.

TWELFTH: On February 18, 2021, the examining body agrees to the am-

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

in article 32.1 of the LPACAP.

The Extension Agreement is notified on February 22, 2021.

THIRTEENTH: On March 8, 2021, this Agency receives, in

time and form, written by the representative of SIMYO in which he alleges and

After expressing what is appropriate to his right, he ends up requesting the file of the proceeding.

proceeding and subsidiarily, that the AEPD consider the mitigating circumstances

substantiated and end the procedure by means of a warning and with the imposition

sation of the obligations to implement suitable corrective measures. In last ins-

If you consider that the imposition of a sanction is appropriate, moderate or modulate the

proposed penalty.

In summary, he argues that:

PREVIOUS.- EXISTENCE OF A WORKING GROUP ON DUPLICATION

OF SIM CARDS LEADED BY THE AEPD.

He argues that the sanctioning procedure has taken place in parallel to the construction

establishment and development of the “Working Group led by the AEPD on Duplication

ity of SIM Cards” in which ORANGE has been participating (in re-

presentation of all the entities of the ORANGE Group, among which are

account SIMYO).

This Working Group (GT) held its first meeting in January 2020 and

born promoted by the AEPD in order to share experiences and analyze the

measures that are being adopted by both sectors (Banking and Telecommunications)

tions) with the aim of minimizing the risks that this new fashion entails.

ity of fraud.

The fact that within the GT the AEPD requires the Group

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, as well as the sharing of a huge amount of information related to

the problems and difficulties encountered by telecommunications operators

cations to control this type of fraud, should lead us to think

that said sharing of information is carried out within the most absolute and strict

strict framework of trust and full confidentiality.

Furthermore, public-private collaborations contribute to the Admi-

de nistration the essential advantage that companies specializing in de-

finished services, provide knowledge and the best solutions in

issues that are of interest to consumers and citizens.

The ORANGE Group has participated and participates today in workshops

with the Ministry of Economic Affairs and Digital Transformation and with the Mi-

Ministry of the Interior.

During 2020, the collaboration with the Security Forces and Bodies

of the State (FCSE) for the prevention or investigation of criminal offences, has

post more than 40,308 requests attended and derived from the Courts;

45,552 requests attended to and derived from the Judicial Police and 50,056 inter-

Telephone conventions carried out (between registrations, cancellations and cessations).

In addition, the company's outstanding collaboration performance has meant

the decoration of the staff assigned to these actions with the Cross to the doctor

Civil rite with white badge, of the National Police and Civil Guard.

Additionally, he has actively participated in the report of the presentation of es-

studies on the risks arising from the use of the network by minors

in the Senate. Likewise, the ORANGE Group has participated 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 to do would be to wait until conclusions are reached on the measures to be taken.
adopt and, once known and put in common, and given an adequate term
to achieve its implementation, it is then, when the operators can be required
regulators that certify its compliance and in case of not having done so, it is
then when sanctions are proposed.
The WG meetings have suffered delays due to the CO-pandemic
VID 19, which has harmed the analysis of the problems associated with these
crimes and, consequently, the proposal and implementation of improvements.
In view of the facts, it seems that the agency has no intention of
mission to comply with the minimum principles of institutional loyalty
that are presumed in any relationship of public-private collaboration, as
at the same time that it is requesting collaboration, information and participation
active and effective participation in the GT, initiates a sanctioning procedure that deals
on the matter dealt with, proposing million-dollar sanctions to all members
industry players who, in good faith, participate in this.
It crosses the most elementary limits of the institutional loyalty that is presumed to
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 the ORANGE Group and the AEPD, and if
they allow it to us, of all the sector of the telecommunications to national level.
For all these reasons, SIMYO wants to record that this way of proceeding affects
seriously violates the principle of trust that the ORANGE Group presumed to be able to
deposit in the AEPD and poses a risk to the objectives of the GT, which will be ob-

subject of internal and probably sectoral analysis regarding the collaborative framework

with Administrative Authorities that pursue this common good of the citizens.

give us with action plans 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

of SIMYO. By itself, this act is not enough to carry out operations

bank accounts on behalf of the initial SIM card holders, but has

of an additional and independent criminal activity to the previous one.

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 SIMYO

He has no decision-making power.

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

types of online platforms.

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

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

security does not necessarily have to be configured in this way, being

This is an option whose choice is up to the bank and/or the user co-

responding.

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

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

online payment".

This fact is more evident if we take into account that the same effect could

also occur without the need for identity theft before an operation

gilds This would be the case in which a subscriber decides to cancel his number

of telephone and this later was object of a portability. If the user

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

three 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).

However, SIMYO is not immune to the problems arising from the potential use

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

ted reinforced security mechanisms in relation to the conditions for

your request. These measures have been increased to the extent that

protects any weaknesses or possible improvements to ensure the security of the pro-

cease.

Furthermore, SIMYO is fully involved as it is part of the WG. action-

tions such as changing the SIM leave a record on the network and it is precisely these

records used by SIMYO to help banking entities in

prevention of this type of fraud.

SECOND. – UNFOUNDED GENERALIZATION OF NECESSARY 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

key sending an SMS with a code to be able to change 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.

tion.

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

SIMYO already has a lot of information to request a duplicate card.

information regarding the interested party, which is necessary for the management of the request of the

duplicate. Therefore, obtaining this information, presumably

illicit mind, is the responsibility of third parties or of the owner of the data,

existing in many cases an imprudent behavior of the latter

in the custody of your personal information.

SIMYO's responsibility cannot extend beyond those matters

tions that fall under its scope of action.

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

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

SIMYO diligence, but rather, performs these operations by requesting data from

who is supposed to be its owner and to carry out verifications, not having

provided any type of personal information that was not initially held by the

bidder.

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

illegally are not obtained from SIMYO, but rather the impersonators obtain them pre-

directly from other sources (the interested party or third parties responsible for di-

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

accompanied by falsifications of public documents, such as copies of DNI or

alleged complaints filed with the police, which are provided as a means

to overcome SIMYO's control measures. It appears in file E/

220/2020, that calls are made in which impersonators pretend to be

sar by SIMYO, providing the client with information about his ID, which in any way

form, the impersonator would not have been able to obtain.

He argues that there is no evidence whatsoever that customer information is not

has been adequately protected.

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

April 2009, of the Telecommunications Market Commission.

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

to criminals having managed to obtain personal data from SIMYO,

Therefore, there can be no question of non-compliance with measures to protect

Personal information.

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.

Of the different sanctioning procedures and file resolutions mentioned

mentioned and whose facts deal with fraudulent actions due to su-

plantations of identity with SIM cards, in none of them is observed

that there is a qualification by this control authority as an in-

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

It invokes article 54 of Law 30/1992, which said: they must be motivated

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

and the SAN of May 13, 2005 and May 7, 2007 (rec: 86/2005). Namely,

that in the event of the same factual assumptions, the application of different solutions

must be justified "with a brief reference to facts and legal grounds"

of the reason for such disparity in order not to undermine the principle of security

legal.

On the other hand, the mention made by the AEPD alluding to the fact that it “appreciates possi-

possible vulnerabilities” in the SIMYO Security Policy “during the phase of

validation of the identity of the applicants of the SIM duplicates”, does not justify

does not in any way qualify the facts.

In this sense, the rationale provided is limited to referring to po-

possible vulnerabilities, which in no case are identified, much less

exposes why they can be qualified as insufficient or inappropriate

quads.

It is also noteworthy, nor is it justified by the AEPD in what

how the privacy of users is affected as a result of the specifics

these actions carried out by SIMYO, but is held responsible

of the effects derived from other actions that do imply a non-au-

to the personal data of those affected, victims of assumptions of

phishing or similar, which do allow access to protected personal information.

given by other data controllers.

THIRD.- SUITABILITY AND COMPLIANCE WITH PREVENTIVE MEASURES

YOU ARE IMPLEMENTED BY SIMYO.

SIMYO has carried out a detailed study of its activities in the treatment of

personal data carried out and has adopted the pertinent measures to

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 identified risks.

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 an Information Security Policy and a governance model

responsible for implementing and operating security, measuring the

control maturity levels and manage risks. The ORANGE Group

maintains and certifies Information Security Management Systems based on

two in ISO27001 and National Security Scheme.

The existing protocols have been communicated to all those involved.

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 of the controls, although hypothetically it could allow a better control

of the procedures, would have an exorbitant cost.

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 state of the art.

uniqueness, the costs of application, and the nature, scope, context and purposes

of the treatment.

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

responsible for carrying out these procedures, which in practice comply with all

quality of the cases with the indications received from SIMYO. Equal-

mind, it also does not take into account the small number of cases in which

a contingency has occurred associated with the request for a duplicate card-

ta, which specifically represents ***NUMBER.6% of cases.

On the other hand, simply pretending that a measure be implemented that automatically

mind cancel a risk is an overly simplistic analysis, which has no

taking into account the context in which the events occur or the complexity of the

management of situations in which a subscriber requires this type of service.

QUARTER. - SIMYO'S DILIGENT PERFORMANCE.

SIMYO has not implemented "static security measures", rather, it has

proceeded systematically to implement improvements in the measures adopted

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

Regarding the content of recital 75 of the RGPD that the AEPD brings to

collation, it must be reiterated that the personal data of the victims are usurped

two prior to criminals approaching SIMYO and that, precisely,

mind as a consequence of having access to personal information that only

should be in the possession of the interested party, allow the impersonation to materialize

of identity.

This circumstance in no way precludes the fact that SIMYO 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 manage to deceive the person who is requested

the duplicate. The possibilities of verifying the documentation provided

are in practice very limited. So this is deception enough,

for having this "appearance of reality and sufficient seriousness to deceive

persons of average perspicacity and diligence” (thus considered, among other

many, in STS 2362/2020).

Occasionally certain partial breaches of the protocols occur

provided by SIMYO, which in certain cases contribute to the achievement

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 SIMYO is inferred as responsible for the treatment

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

On the contrary, the measures implemented are adequate to mitigate, in a

majority, the risks related to this type of fraud. In practice, such

and as reported, the efficiency of these measures is close to 100% of the

cases.

It must be remembered that there are combined safety factors that make it difficult

the target of fraudsters. In this sense, the protocols include

the different measures adopted depending on the means by which the request is made.

duplicated and in the subsequent phase of delivery and activation of the SIM.

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

SIMYO by those involved in the processing of applications, has been

produced the impersonation result.

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 SIMYO, it has been proven that:

- It has established adequate protocols for the prevention of impersonations

of identity in the process of requesting duplicate cards.

- It has duly communicated the content of these protocols and the obligations

corresponding to the people involved in the processing of these applications.

applications.

- Has made improvements to processes when 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

the SIM Swap system launched in October 2020).

- Has acted as diligently as possible, promptly, efficiently

and executive, in the cases in which there has been knowledge of any

cho related to identity theft.

- It has systems to verify compliance with its obligations

by the people involved in carrying out the application processes.

number of duplicate cards.

Furthermore, it is reported that recently the complaints filed

sit-ins for this type of crime are beginning to yield results

relevant in the form of arrests.

Consequently, SIMYO's activity cannot be classified as negligent.

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

It invokes the STS 1232/2018 of July 18, 2018. Thus, in accordance with the criterion

of the Supreme Court, SIMYO could not be held liable even if his company

employee or collaborator had been negligent in his action, since it was required

would laugh "culpable or malicious actions" on his part, which under no circumstances

it has been produced.

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, it considers that the jurisprudence analyzed supports the

SIMYO's behavior, having established an ele-

prepared taking into account the existing risks, which was made available

of all those involved and that, if they had been followed, no action would have been taken.

assigned to the delivery 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 SIMYO by the AEPD itself.

FIFTH. – LACK OF PROPORTIONALITY OF THE PROPOSED PENALTY.

There has been no breach of data protection regulations,

since SIMYO has taken all the necessary technical and organizational measures.

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

The proposed sanction is in any case disproportionate, taking into account the circumstances

Cunstances and content of the alleged infractions.

As for the number of existing cases that the Agency considers to be welcome,

vant, there are three of them and they have an excellent capacity for reaction, as well as

preventive and corrective measures.

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

hold SIMYO accountable for situations related to the use of duplicates

of the card that derive from information security incidents with the

that SIMYO has no relation. Card duplication does not derive di-

correctly, nor necessarily, in fraudulent banking operations, since

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

Banking operations are totally unrelated to SIM card duplication.

For all of the above, the alleged damages indicated by the AEPD

they could not be imputed to SIMYO nor, therefore, be considered an aggravating circumstance.

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

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

of the sanction.

On the degree of responsibility: they have been detailed throughout the requirement.

of information the many measures adopted, as well as the improvements that have been

been introduced, including the impossibility of allowing address changes.

sending tion during a SIM change/duplicate request. Highlights the eli-

Elimination of the possibility of requesting duplicate SIM cards at Points

of Sale, dated August 23, 2019, as well as through the Personal Area

(eCare) or through the App. Likewise, it is interesting to highlight the Plan of

action in SIMYO to achieve the necessary technological developments and improvements

so that requests for change of postal address, email, between

other contact details, are verified by means of a certified SMS.

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. This does not mean that the impersonator can operate on behalf of the

affected, unless the security measures of other entities have been bypassed.

data, such as those of the bank.

On the other hand, with respect to mitigating factors, although it includes the existence of

palliative measures, it omits any preventive measures implemented by SIMYO.

All this means that the attenuation must be higher. Likewise, it is considered

the lack of economic benefit obtained by SIMYO. However, it has

to highlight that SIMYO is one more victim of the criminal network carried out

by the supplanters.

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

SIMYO's guilt, in the event that it is considered that there is some kind of

infraction, the proposed economic sanction included in the Initiation Agreement

should be replaced by the adoption of corrective measures (article 58

RGPD), consisting of the warning or warning to the person in charge and the im-

position of the obligation to adopt measures to carry out the treatments

cough “in a certain way and within a specified time”.

FOURTEENTH: On April 27, 2021, this Agency receives a written

of the representative of SIMYO by which he adduces additional arguments to the above

above and attach the following documentation:

OF A GENERAL NATURE:

- Document 1: (...)

- Document 2: (...)

- Document 3: (...)

- Document 4: (...)

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.

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

initiation and presented allegations, on April 30, 2021, the instructor of the

procedure agrees to the opening of a period of practice of tests, notified to

SIMYO on May 4, 2021, in the following terms:

“The claims filed are deemed reproduced for evidentiary purposes.

rates by C.C.C. and A.A.A., their documentation, the documents obtained and generated

generated by the Inspection Services before ORANGE ESPAÑA VIRTUAL,

S.L., and the Report of previous inspection actions that are part of the

file E/11418/2019.

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

to the initiation agreement PS/00046/2021 presented by ORANGE ESPAÑA

VIRTUAL, S.L, on March 8, 2021, through the General Registry

of this Agency, and the documentation that accompanies them:

Document 1 (…)

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

“complementary” to the initiation agreement PS/00046/2021 presented by

ORANGE ESPAÑA VIRTUAL, S.L, on April 27, 2021, through the Re-

General Registry of this Agency, and the documentation that accompanies them.

na:

- Document 1: (...)

- Document 2: (...)

- Document 3: (...)

- Document 4: (...)

- Document 5: (...)

- Document 6: (...)

SIXTEENTH: On October 7, 2021, the instructor of the procedure

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

ORANGE ESPAÑA VIRTUAL, S.L., with NIF B85057974, is sanctioned for infraction

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 70,000.00 (seventy thousand euros).

ros).

On October 14, 2021, through the Citizen Folder, the Pro-

Resolution setting.

SEVENTEENTH: On October 19, 2021, SIMYO requests the extension

of the term to formulate allegations to the Resolution Proposal.

EIGHTEENTH: On October 20, 2021, the Agency agrees on a

extension of the term to present allegations in one more business day, that is, until the day

October 29, 2021.

NINETEENTH: On October 29, 2021, SIMYO, makes allegations to

the Resolution Proposal in which the allegations are ratified and reproduced.

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

MO THIRD and FOURTEENTH) and also adds others:

FIRST: INFRINGEMENT.

It shows that in the Background and in the Proven Facts of the

The Agency's Resolution Proposal mixes and confuses the two assumptions

in fact of the two claims.

In the same line, both claimants are associated in the Background with the email

***EMAIL.1, when it is obvious that said email address only corresponds to one

of the two claimants.

These facts cause an obvious helplessness to SIMYO, who cannot discern

clearly define the account of the facts to impute an alleged infraction.

It is noteworthy that in the FD the commission by the

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

for tested. This, before even trying to justify the reason. This pro-

yielding, even if only to formal effects, is legally inappropriate and

could be considered a certain predisposition of the AEPD to sanction it, regardless

pending the allegations that can be made in his defense, given that

no such violation has occurred.

SECOND: TREATMENT OF PERSONAL DATA AND RESPONSIBLE FOR THE

TREATMENT.

A series of clarifications are required in relation to the fact that the duplication process

do of a SIM card involves the processing of personal data.

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

identification formation of the holder of the line, not the technical information contained in

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

own phone number (preceded by the country code).

These and not others are the data object of treatment carried out by SIMYO in cal-

responsibility.

All this information was already known to criminals prior to requesting

cite the duplicate, after having previously obtained them illicitly through

social engineering techniques such as “phishing” or “spoofing”.

Therefore, the statement that "SIMYO is responsible for the

processing of data referred to in the exposed antecedents”, since in the same

We refer to other treatments that are not your responsibility.

There is no evidence that any information has been processed by clients that could be

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

the phone list or the calls and messages list. Regarding the IMSI, there is no

No proof or indication that this data has been processed for any purpose.

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

It 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,

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

possibility of identification by third parties other than the operator required

additional information that is not available, so even in the event of qualification

consider them as personal data, they would be considered pseudonymised data.

do.

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 SIMYO's performance.

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 SIMYO's performance, it does show the recognition of the problem

existing matic and the difficulty posed by its prevention: it is a pro-

generalized and recurrent problematic, which affects multiple entities and opera-

telecommunications providers whose solution is highly complex and, although

has shown the joint will to put an end to these assumptions, eradicate

it is a difficult objective, given the ability of criminals to

to update their techniques and deploy increasingly sophisticated means.

fallen to achieve their goals.

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

MYO, 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 SIMYO other than that provided by the pro-

pio delinquents obtained through social engineering techniques such as

“spoofing” and “phishing”, therefore, SIMYO has not allowed access by third parties.

unauthorized parties to personal information to which they do 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 SIMYO 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

SIMYO are mere speculations, which refer to potential risks

them, 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 the punctual overcoming by a third party – ter-

zero, that we must identify as organized criminals, with high knowledge

computer skills, and an elaborate modus operandi in which, among others,

use social engineering techniques - to a lack of security, without evaluating the ni-

speed of diligence deployed by SIMYO.

SIMYO only recognizes that it is necessary to implement new measures

before the commission of this type of fraud, and it is precisely this model

management, continuous improvement, in accordance with the spirit of the RGPD and article 5.2,

(as the Agency itself has recognized), which means that SIMYO has not co-

committed any infraction in their treatment of personal data, because they have been

Appropriate security measures have been deployed, subject to review and

jora.

Regarding the improvement of protocol compliance controls, if

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

No matter how tight the control or monitoring of your activity is, always

there is a possibility of non-compliance. Thus, for example, it is not possible

control whether or not a manager has asked a specific question to a client,

or verify that the answer is correct. Just as a user

authorized person always has the option to reveal confidential information of the

have knowledge.

In relation to the two duplications of SIM cards, these are due to a

inadequate application of the protocols established by SIMYO.

It should be remembered that, in addition, in both cases the security measures are exceeded.

security because the impersonators knew the personal data of the claimants.

blankets.

In relation to the statements contained in the Seventh Proven Fact, on-

on alleged inconsistencies between the “Security Policy” and the “Documentation
Duplicate SIM”, it should be noted that they are not exclusive
rather they complement each other: although both documents are addressed to
agents that process requests in the Call Center, the document “Documenta-
Duplicate SIM” is prior to the “Security Policy”, although it is
only for a few days. That is why the most recent document,
(the “Security Policy”) is the one that strengthened the security protocol and
incorporated the ICCID or PUK application requirement together with the DNI, as a measure
additional days of guarantee of identity. This new protocol takes into account
assessment four levels of risk, in which the type of request of the
client, being, precisely, the request for a duplicate SIM card the act
to which a critical risk was assigned in said document, established
thereby taking additional measures to those already provided for in the previous document.
river.
In relation to the differences between points 4 and 5 of “Documentation Du-
SIM plicate” and the document “New Management Model”, indicate that the last
mo is dated 2019, so it predates all other documents
mentioned. The difference in this case is derived from the context of emer-
health and pandemic agency that took place in March 2020: although in
2019 the document "New Management Model" collected the impossibility of mo-
dify the delivery address of the SIM card, the situation during the spring
2020 forced to modify all procedures, and, among them, enabled
tó the possibility of modifying the delivery address. The post-
later “SIM Duplicate Documentation” allowed address changes from
shipping as long as it was in the same province. This change is justified
affected by the impossibility of delivering the order in the work centers and in

Points of Sale during the health emergency.

Thus, the information collected in international procedures is decontextualized.

SIMYO with the intention of identifying contradictions, when, in reality,

Indeed, these nuances are only due to the different time frames

in which the various documents are issued.

4. THIRD ARGUMENT. – SUITABILITY AND COMPLIANCE WITH THE MEASURES

PREVENTIVES IMPLEMENTED.

The AEPD questions the protocols that SIMYO uses. However, the arguments

The arguments he uses to make this statement are contradictory.

Therefore, following the effectiveness criterion pointed out by the AEPD itself and even

that what is desirable is always to achieve the cancellation of the risk, the percentage that

present the cases, ***NUMBER.4%, does not allow to qualify the protocols as

inappropriate.

The risk approach introduced by the RGPD comes to determine that, given the impossibility of

possibility of a zero risk, the appropriate measures will be those that, within the

state of the art, application costs, nature, scope, context

and the purposes of the treatment, allow to reduce the risk inherent to the minimum risk

possible.

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

has produced an undesired result supposes adopting a principle of responsibility

objective ity in the sanctioning scope vetoed by our Legal System.

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, that is, the

possibility of answering "... even as a simple non-observance".

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

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

tion, when sanctioning, prove some degree of intentionality. It requires the

recurrence of guilt in the degrees of intent and fault or gross negligence, not

Mere negligence is sufficient.

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

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 evident indepen-

fension, he does not know with certainty what to expect, nor what measures can be implemented,

when they are considered appropriate on certain occasions, and, on others,

constituting a very serious offence.

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

measures, an adequate level of diligence is appreciated and, nevertheless, in the present

procedure, where only two interested parties have been affected, no

assess as adequate the level of diligence shown, through the measures of

security, detection and correction, taking into account the number of security processes

SIM duplication made.

SIMYO is also the victim of an “attack” led by criminal organizations

that has digital and social engineering techniques aimed exclusively at

overcome the security measures implemented.

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

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

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

Any agent could accept the buttons to continue the process despite not

having carried out the specific security measure.

The full employee monitoring options, in addition to not being provided

tioned in accordance with the data protection regulations, they would have a discounted cost.

proportionate, considering that it should be exhaustively controlled to all the

agents potentially involved in an operation of this type (maximum

taking into account that the control should be carried out in real time), when the

Statistics show that the related incidences are negligible.

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

necessary information and that the information and management is carried out without any impact on

practically all cases.

Additionally, it is possible to verify compliance with the obligations, since

that user activity is recorded.

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

ity, SIMYO continues to analyze possible improvements in all its processes.

Regarding the contractual documentation with the delivery companies, it should be noted

that in the two cases that concern us, no company or

delivery service provider.

The certificates that SIMYO holds, as part of the Orange Group, recognized

by the National Security Scheme (ENS), have a broad scope, which does not

only encompasses information systems, but there are a series of

controls that apply to the entire organization, in attention to different aspects,

inclusive: data protection, 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 evade responsibility, what is requested is precisely that

Such responsibility is limited to the treatment actually carried out, without extending the

responsibility corresponding to other entities, such as operations and

actions carried out by different banking entities.

Lastly, it should be noted 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 SIMYO, nor the consideration of the tiny percentage of incidents that have been

produced in the SIM card duplication processes.

5. FOURTH ARGUMENT. – DILIGENT PERFORMANCE BY ORANGE.

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

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

considering 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 of

integrity and confidentiality.

He emphasizes the contradictions of the Agency and invokes that it makes him totally defenseless.

sion, because despite the fact that it has managed to prove in the procedure the

fulfillment of his duty of diligence and being recognized, is the subject of a

sanction for an undetermined reason, before which you cannot present

try any.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

33/88

All this brings cause in that the AEPD is evaluating the responsibility of SIM-

I attending only to one result, constituting an assumption of res-

objective responsibility, being indifferent to the diligence displayed in his

preventive and palliative measures.

Reasons why they should be discarded:

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

imposed by the RGPD […] does not impose in any case the infallibility of the

measures (…)". However, it intends to sanction for two specific cases

among nearly a million.

• Regarding the impossibility of verifying the DNI in the case of the complaining party-

two, despite having specific software, it is an impossibility

technical reliability, not an error in the security procedure.

•

•

•

It indicates that the fault has to do with the diligence displayed, not with a hero.

cho objective as the number of processed data.

“The infraction occurs not because of the lack of a specific security policy.

ity for the issuance of SIM duplicates, but because of the need for their revi-

sion and reinforcement”. Despite having recognized that, “SIMYO has acted diligently

when it comes to minimizing the impact on those who may be affected by implantation

new security measures to avoid the repetition of similar incidents.

res in the future".

• The AEPD re-introduces a new criterion for the responsibility of SIM-

I in the cases analyzed, indicating that it "is directly related to

related to the generation of consequences in third parties". Move to SIMYO

responsibility for treatments over which it has no capacity.

control.

• The concept of improvement, abstract and generic to which the Agency alludes, would allow

classify any protocol as inadequate, insofar as any process is sus-

room for improvement.

It includes certain jurisprudence related to fault, in which it is recognized

that it does not attend if it is justified "that the due diligence has been used

demandable by the person who alleges its non-existence" or it is indicated that "there is no negligence

ence, nor therefore infraction, "when the necessary diligence has been put in

fulfillment of obligations".

• The liability of a legal person must be assessed based on the di-

ligence deployed as an entity, manifested through the procedures

and instructions approved by it.

However, the AEPD does not consider that the risks generated by third parties

(banking entities) and that are their responsibility, would be mitigated in a

much simpler if they adopted adequate measures to improve security.

the nature of the operations they perform.

Reasons why SIMYO should not be sanctioned:

The confidentiality of the data processed in the duplication process of the tar-

jeta SIM was previously broken by banking entities.

SIMYO has no control over this operation nor can it affect its authorization/provision.

assignment/execution.

The succession of suppositions and possibilities cannot serve, under any concept,

to, as a justification, to impose an infraction on SIMYO without entering into an assessment,

reasoned, the level of diligence displayed and the events that actually occurred

two. These threats identified by the AEPD fall outside the scope of action

tion of SIMYO.

The AEPD considers guilt of SIMYO's conduct, although, far from identifying and relating

tar the concrete behavior, is limited to referring to the result. This procedure is not

in accordance with current legislation, as indicated by the National High Court, among others,

in the Judgment of the Contentious-Administrative Chamber, Section 1, of 23

December 2013, Rec. 341/2012:

It should be remembered that the reference to "simple non-compliance" has been removed

by the current Law 40/2015, for which a lack of qualified diligence would be necessary.

each.

Invokes the SAN, Contentious Chamber, of February 25, 2010, Appeal No.

226/2009".

Mere human error cannot give rise, by itself, to sanctioning consequences.

swimmers.

The similarity of this case with the one included in the SAN of

February 25, 2010: these are intrusions committed illegally, for

zeros organized and with high computer knowledge, directed to an activity

highly elaborate crime.

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

dere that his diligence does not include having the capacity to repel this type of attack.

ques is interpreted in the opposite way in this case, penalizing SIMYO because

their security measures may depend on the actions of specific people.

you.

SIMYO, nor its employees or agents, may not be required to have the ability

to infallibly identify cases of fraud, especially when

offers, an “appearance of reality and seriousness sufficient to deceive people

of average perspicacity and diligence” (so considered, among many others, in the

STS 2362/2020).

6. FIFTH ARGUMENT. – LACK OF PROPORTIONALITY OF THE PENALTY

PROPOSAL.

Despite the fact that the AEPD has modulated the amount of the sanction imposed, it is considered

It is believed that, having been diligent in their actions, no imposition of sanctions is appropriate.

any tion.

For the hypothetical case that the existence of an assumption incompliance is considered,

compliance, it is not proportional.

It should be stressed that no dissuasive action is necessary, as long as the

position object of the present procedure has been carried out against all

volitional element of SIMYO.

SIMYO has not obtained any benefit, but it has been a detriment. By

which, as far as the need for the deterrent effect is concerned, the mere commission

of the crime is detrimental to SIMYO.

Additionally, it participates voluntarily in the GT.

FOURTH.- PRINCIPLES RELATED TO TREATMENT.

SIMYO. shares with the Agency the relevance of security measures in

In order to guarantee the fundamental right to data protection, however,

A series of qualifications must be made:

The damage suffered by both claimants has been recognized: both

•

received compensation from SIMYO.

•

Particular circumstances of the claims cannot be considered

presented nor assumptions within the object of this procedure,

the assumptions and possibilities that the AEPD elucidates: access to applications, use

of social networks, etc.

Said assumptions can in no way justify the Resolution Proposal

•

from the agency.

SIMYO has no control over such procedures and has no influence on the

•

security measures used by banks.

•

Although SIMYO., as the data controller, has the obligation to declare

terminate 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.

tions of the first and fails to comply with the purposes and means of the treatment in question, as

This is stipulated in article 28.10 of the RGPD.

•

To reiterate, that on two occasions the identity of the

claimants in two SIM card duplication procedures out of a total of approx.

***NUMBER.3 duplication procedures, by sufficient deception

cient, it cannot automatically determine the commission of infraction and absence

of diligence on the part of SIMYO.

SIMYO does not "provide duplicate SIM cards to third parties". How-

•

If the third party got the duplicate SIM card, it 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. There is also no evidence of access by supplanted

identity agents to personal data other than those that they already knew in a

ra prior to fraudulently obtaining the duplicate SIM card.

•

In relation to STC 292/200, the definition and consideration

tion 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.- SECURITY OF TREATMENT.

The legal classification made by the Agency of the infraction imputed to SIM-

YO does not include the violation of article 32 of the RGPD.

SIXTH.- GENERAL CONDITIONS FOR THE IMPOSITION OF THE FINE AD-

MINISTRATIVE.

The treatment carried out does not violate data protection regulations, since,

SIMYO has displayed an appropriate level of diligence in imposing the measures

technical and organizational measures necessary to prevent the commission of fraud in the

requests for duplicate SIM cards.

The proposed sanction is in any case disproportionate, taking into account the circumstances.

substance and content of the alleged infractions.

Recitals 11 and 13 of the RGPD, which refer to guaranteeing the protection

effective disposal of personal data and to do so in a consistent manner, point out that

This objective also depends on “infractions being punished with sanctions”.

n equivalents”.

- Aggravating factors:

1. Nature and seriousness of the infraction:

The loss of control and disposal of personal data does not start when

SIMYO performs the SIM duplication, but it takes place before.

The reference to “After the entry into force of the PSD2 Directive, the telephone

mobile begins to have a very important role (...)” does nothing but certify the transfer

responsibility towards SIMYO that the AEPD intends, without taking into account

that the limitation of these risks corresponds to those bound by said regulation.

tive, who are obliged to implement adequate measures, among which

that the confirmation of the operations is not found by sending

SMS.

This section does not assess the nature and seriousness of the offense charged.

tada, which refers to the maintenance of adequate security of the

personal data (article 5.1 f) RGPD), but returns, once again, to

analyze the subsequent activity carried out by the individuals who supplant the

identity of the claimants.

Categorize the nature and seriousness of the treatment carried out by SIMYO,

ge evaluate the security measures established in the procedures of

SIM card duplication.

Reiterate, again, that third parties have not had access to either

assumptions that here concern us with the mobile phones of the claimants,

and, consequently, neither to the information that they could store.

to store, which is different, in any case, from the information that can be stored

add a SIM card (as we have already mentioned, no applications are stored)

nes, for example).

2. Level of damages suffered:

SIMYO is not responsible for the identification and verification policies of

customers established by banking entities.

The Agency indicates that, if the duplicate of the SIM card is not obtained by the

identity theft, it would not have been possible to carry out the banking operations

fraudulent charges and access to the verification system. Nor would

banking operations could have been carried out if the financial entity used

another security system at checkout.

The Agency does not assess the level of damages, as long as it is

limit to indicate that these "multiply", without explaining what is the relationship between

this affirmation and the facts object of analysis in this proceeding.

In relation to the origin that it indicates to carry out an evaluation of im-

pact, the Agency cannot pretend that the possibilities of com-

ssion of fraud in carrying out banking operations through applications

tions and third-party electronic banking. Again, the Agency performs a

simplistic approach, omitting the complexity of the sequence of events.

It cannot be affirmed that the SIM card duplication process derives addresses

strictly, nor necessarily, fraudulent banking operations.

SIMYO has also acted, in a matter of minutes, specifically, in case

of the complaining party two, in 36 minutes it has blocked the SIM, identified the

case and frustrated the offenders' ability to commit further harm.

cio. However, instead of considering the level of effectiveness deployed, im-

places an obligation of absolute result.

For all of the above, the alleged damages indicated by the AEPD

they could not be imputed to SIMYO nor, therefore, considered as aggravating.

3. Intentionality or negligence in the infringement:

The Agency requires SIMYO an absolute obligation of result, as long as the ni-

level of diligence is not being evaluated in attention to the measures and procedures

established procedures, but only attends to the result obtained.

Thus, it introduces strict liability rejected by our Constitutional Court.

institutional, as we have already indicated, in the jurisprudence that emanates from the STC

76/1990 of April 26.

In addition, the Agency also contradicts the jurisprudence (Sentence of the TS

of January 23, 1998) that she herself has been using to support her

legal qualification.

That is why it cannot be considered negligent, as long as

appropriate procedures have been established, which have been reviewed and

progressively forced. In any case, SIMYO must be considered diligent.

people and act this fact as mitigating the sanction.

4. Degree of responsibility of the person in charge:

It should be noted in this regard that in the two cases that concern us, the

agents breached SIMYO's security policy and the specific measures

tas that it imposed.

In addition, as we have been indicating, SIMYO has preventive measures,

technical and organizational measures, palliative and coercive measures, by which

It mentions those who do not comply with the imposed obligations.

Thus, it should be interpreted in favor of SIMYO.

5. 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.

The theory that the SIM card is a personal data has no support.

Therefore, the type of data being processed must be considered as

a mitigation.

6. Linking the activity of the offender with the performance of treatment

personal data:

The activity carried out by SIMYO cannot be considered, in a general way,

neric, as an aggravating element. Otherwise, any procedure

SIMYO would always have said aggravating circumstance, since it is being considered

that the seriousness of a possible infraction is increased by the mere fact of per-

have the telecommunications sector and carry out data processing.

- Mitigators

1. Degree of cooperation with the supervisory authority

In addition to cooperation and collaboration with research, this part wants

I will review the work of SIMYO, as well as of the entire Orange Group, participating

voluntarily in the WG for the review and coordinated improvement of the procedures

procedures related to security in the processing of personal data.

2. The profits obtained as a result of the commission of the in-

fraction

Insist that not only does the absence of benefit occur, but that it has

put a detriment on SIMYO, who has had to carry out investigations

internal complaints, make compensation to the complainants and reevaluate procedures

ments and protocols.

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

SIMYO's fault, in the event that it is considered that there is any type of in-

fraction of the RGPD, the sanction proposal should be replaced by the adopt-

tion of corrective measures (article 58), consisting of the warning or

warning to the controller and the imposition of the obligation

of adopting measures to carry out the treatments “of a certain

manner and within a specified period.

In this regard, SIMYO understands that the initially estimated fine may

to be perfectly replaced by the obligatory adoption of corrective measures.

bulls.

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 from SIMYO any additional personal data to

those who already had prior to going to SIMYO, obtained from entities

banks and that are used to supplant the identity of those affected,

Therefore, the treatment carried out does not imply a breach of confidentiality.

ness of personal data.

3º.- The responsibility of the teleoperators cannot reach the opera-

banking operations that may be carried out as a result of the measures

security measures of banking entities are inadequate.

4º.- It has been proven that the two assumptions are due to an inadequate

application of the protocols established by SIMYO that, as evidence

statistics, are adequate and efficient and only in an absolutely correct way.

sidual 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 scope vetoed

by the 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.

(Bold italics is from SIMYO).

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: SIMYO is responsible for the data processing referred to in the pre-

this Resolution, since according to the definition of article 4.7 of the RGPD it is

who determines the purpose and means of the treatments carried out with the purposes

indicated in its Privacy Policy, among others: For the fulfillment of the relationship

commercial or institutional: those necessary to carry out the provision of the

telecommunications services, maintenance and management of the relationship for purposes

to comply with the provisions of the contract signed between the parties: manage the

User registration and allow access to the activities and tools available to

through the website www.simyo.es; carry out the User registration, as well as the maintenance

maintenance and management of the contractual relationship with SIMYO; 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.-

simyo.es, etc.

SECOND: SIMYO is an integral part of the ORANGE Group (ORANGE, JAZZTEL,

MOBILE REPUBLIC, AMENA and SIMYO).

THIRD: On September 2, 2019, this Agency has entered a re-

claim made by claimant one (file with reference no.

E/10534/2019), directed against SIMYO, after being issued on August 14, 2019,

a duplicate of the SIM card of the line ***TELEFONO.1, in favor of a third party

sona different from the owner of the line -the claimant party one- and be left without service.

At 9:35 p.m. on August 14, 2019, the claimant one receives in his

private email an email from ING DIRECT, where it reads:

“ORANGE LOAN DOCUMENTATION”, “Dear A.A.A., thank you for

choose us for contracting your loan (...) we attach the documentation

legal document relating to the orange loan number ***PRÉSTAMO.1, as well as three

documents in pdf format, European standardized information, assistance prior to

contract, and orange loan contract”. The loan amounts to 43,000'00 euros

with a monthly fee of 586.09 euros, in 84 installments and expiration date

8/36/2026, at 3.95% interest.

At 9:43 p.m. on August 14, 2019 (…) you receive in your email

(...) an email from the ING DIRECT bank, which reads:

“Dear Mr. A.A.A., (…) we enclose a copy of the documentation related to your

hiring (...) contracted product payroll account number ***ACCOUNT.3, where

Likewise, all the personal data of this party are recorded (...)”. From this

payroll account, a transfer is made for an amount of 10,000'00 euros in favor of

a third.

A bank transfer is also made, for an amount of 10,000'00 euros, from

the current account of the complaining party one ***ACCOUNT.1 (ING) to the account

***ACCOUNT.2 (BBVA) -of which his wife is the owner-, without his consent.

There is a telephone call from the line ***TELEFONO.1 to the number 912518375 to

at 10:36:22 p.m. on August 14, 2019, to the BBVA Customer Service Department.

Due to these facts, claimant one files a complaint with the Unit

Organization of the Judicial Police of the Civil Guard, Huelva Command, on date

August 15, 2019, with proceedings number XXX/XX, which is subject to

extension, dated August 21, 2019, in which it adds:

“(…) That the creation in the positions of the undersigned of the entity

banking ing,

Debit card in the name of A.A.A. ***CARD.1

Debit card in the name of A.A.A. ***CARD.2

Credit Card in the name of A.A.A. ***CARD.3”

The complaining party one, on August 15, 2019, contacts SI-

MYO, through Customer Service, indicating that it does not recognize either the du-

SIM card application or modification of contact details (email)

done.

SIMYO confirms that the SIM card was delivered on 08/14/2019 in a (...) and

that the activation occurs through the (...) through the option existing in that

moment of “(…)” at 21:15:40.

The activation is carried out after (...).

SIMYO, dated August 23, 2019, eliminates the possibility of (...).

SIMYO, dated August 30, 2019, disables the possibility of (...).

SIMYO acknowledges that (…).

FOURTH: On November 6, 2019, this Agency has entered a re-

claim made by claimant two (file with reference no.

E/00220/2020), directed against SIMYO, after being issued on August 23, 2019,

a duplicate of the SIM card of the line ***TELEFONO.4, in favor of a third party

sona different from the owner of the line - the complaining party two - and be left without service.

On August 23, 2019 at 5:02 p.m., the complaining party sends an email

email to "soporte@simyo.es" with the following tenor:

"Buenas tardes,

I need to know the data of the phone that has called me with a hidden number

pretending to be a SIMYO operator to obtain my personal data.

Last call received:

Day: 08/23/2019

Time: 16:12

Duration: 1 Min 13 sec

I enclose my ID, as indicated by the customer service operator for

get this information.

Thanks in advance.

C.C.C.”

On August 24, 2019, the complaining party two, accesses the Personal Area of

client and see the following message:

“Here you have the history of all the operations carried out with your lines

(portability, registration, shipping...) 08/23/2019 17:48:43 Mission accomplished! I already

we have delivered your duplicate sim, remember that to activate it go to

DUPLICATE/ACTIVATE SIM section of the menu. LINE: ***PHONE.5."

Due to these facts, claimant two files a complaint with Post P.

of Rincón de la Victoria, of the Malaga Civil Guard Command, on the date

August 24, 2019, with report number *** COMPLAINT.1 in which it states:

"(…) who is the owner of a bank account in the entity Banco Santander with

account number ***ACCOUNT.4, in which it appears as authorized persons

the complainant's father D. E.E.E., his mother Dª F.F.F. and the brother of

complainant D.G.G.G..

That on August 23, 2019, around 10:45 p.m.

complainant accesses the account inquiry application of the Bank entity

Santander, and you can check how the amount of

30,000-- euros, who immediately makes a phone call to his parents

to find out the reason for said withdrawal, and that his parents inform him that they do not

have made no movement of that amount. (…)

That the complainant receives a call on his mobile terminal with a number

***TELEFONO.4, which operates with the company SYMIO, with a hidden number and

privately, around 1:35 p.m. approximately, in which a

male interlocutor, several questions without being related to the

complainant, such as providing your ID, date of birth, etc., that the

interlocutor had a Spanish accent, apparently from the north of Spain.

That the complainant receives a second call with a hidden and private number in

the aforementioned terminal, at 4:12 p.m., on August 23, 2019, in the

which the male interlocutor tells him: Hi, I'm calling from SIMYO, (offering him a

offer of data and calls), requesting the complainant his date of birth,

providing the interlocutor with his date, the interlocutor informing the complainant

that if he wanted to verify the offer he should call the number 1644, customer service number

to the customer of SIMYO company.

That the complainant makes a call to 1644 to verify the veracity of the

offer and is informed that the company has not offered him anything. (…)

That the complainant sends an email to the aforementioned company to

report what happened.

That the complainant checks how his mobile terminal is left without coverage,

contacting the SIMYO company again to find out the reason for this

incidence, being informed by the company, that it did not have coverage due to

of security, and that on Monday the problem would be solved.

That through the personal area (...), you can see a message, at 04:57

hours day 08-24-2019, in which it is stated that there has been a duplicate of the

SIM card, which occurred at 5:48 p.m. on 08-23-2019, being of

special interest since this duplication takes place approximately one hour,

that the complainant inform the company of the calls received with

hidden and private number.

ASKED to say or provide the information available to the

extraction of the amount of 30,000 euros.

STATES that it has occurred through bank transfer, which does not

has not been authorized by the complainant, nor has it proceeded to enter codes of

confirmation, nor make the electronic signature, not knowing how it has been possible

produce said transfer, that the account where the money has been transferred is

the following ***ACCOUNT.5 where Hhh (sic) appears as the beneficiary, you cannot

provide an extract of the movement, since the entity is closed due to the end of

week, and not being able to access your current account through the application of

the entity for having the mobile phone blocked".

In relation to this claim, SIMYO verifies to this Agency that, on the 23rd of

August 2019, (…).

On 08/23/2019 at 18:24:34, SIMYO proceeds (...).

At 7:47:04 p.m. that same day, there was a (…).

SIMYO confirms that (…).

SIMYO confirms up to a total of (…) ***PHONE.6 and ***PHONE.7 and confirms

than the person who (...). It also confirms the receipt -on that same date- of (...)

from the numbers ***TELEFONO.8 and ***TELEFONO.6.

FIFTH: In December 2019, SIMYO informs the AEPD of the security policy

applicable to requests for duplicate SIM cards and distinguishes

(…)

SIXTH: SIMYO has a Security Policy (...)

SEVENTH: SIMYO has security measures that it applies to the process of

issuance of the duplicate SIM collected in the (...).

EIGHTH: SIMYO has defined a new (...), which provides the following instructions

nes:

(...).

NINTH: SIMYO has security measures that it applies to the process of

"(…)" that includes the following instructions:

(…)

TENTH: SIMYO has a system of (...)

ELEVENTH: (...)

TWELFTH: SIMYO is an integral part of the ORANGE group, which is part of the

Spanish Association for Digitization and participates in the project "Digital Identity

Segura (IDS)" whose purpose is -among others, to protect against fraud and cyberattacks-

ques and the defense of data privacy.

It actively participates in the proposal of different driving projects and in the development

llo of applications that guarantee the IDS.

(…)

THIRTEENTH: SIMYO has adopted a series of actions to prevent SIM

Swapping:

(…)

FOURTEENTH: SIMYO reports (...) ***PHONE.9 and ***PHONE.10 respectively

tively, canceled in both cases.

There is a recording related to the activation of a SIM card on the line ***TE-

LEFONO.9 in which (...).

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 SIMYO 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 SI-

MYO, identifying the vulnerabilities that could 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 SIMYO has a security policy

security in which the way of acting in the face of personal data processing is established.

personnel necessary for the issuance of duplicate cards. However,

It was also proven that adequate safety in the work had not been guaranteed.

impersonation of personal data, taking into account the result produced by the impersonation

tion of identity

The concept of proactive responsibility is linked to the concept of compliance.

regulatory enforcement or compliance, already present in other regulatory areas (we refer to

We refer, for example, to the provision of article 31 bis of the Penal Code).

Thus, article 24 of the RGPD determines that “1. Considering the nature, the

scope, context and purposes of the treatment as well as the risks of different probabilities.

ity and seriousness for the rights and freedoms of natural persons, the person responsible

of the treatment will apply appropriate technical and organizational measures in order to guarantee

czar and be able to demonstrate that the treatment is in accordance with this Regulation. Gave-

These measures will be reviewed and updated as necessary.

2. When they are provided in relation to treatment activities, between

the measures mentioned in section 1 shall include the application, by the res-

responsible for the treatment, of the appropriate data protection policies”.

Proactive responsibility implies the implementation of a compliance model and

management of the RGPD that determines the generalized fulfillment of the obligations

in terms of data protection. It includes the analysis, planning, establishment

maintenance, updating and control of data protection policies in

an organization, especially if it is a large company, -understood as the set-

set of guidelines that govern the performance of an organization, practices, procedures

and tools, among others-, from privacy by design and by default, which

guarantee compliance with the RGPD, that prevent the materialization of risks and

that allow the controller to demonstrate compliance.

Pivot on risk management. As established in Report 0064/2020

of the Legal Office of the AEPD shows the metamorphosis of a system that has

gone from being reactive to becoming proactive, since "at the present time,

It must be borne in mind that the RGPD has meant a paradigm shift when approaching

give the regulation of the right to the protection of personal data, which becomes the foundation

be based on the principle of "accountability" or "proactive responsibility" as

The AEPD has repeatedly pointed out (Report 17/2019, among many others) and it is re-

takes in the Statement of Reasons of the LOPDGDD: "the greatest novelty presented by the

Regulation (EU) 2016/679 is the evolution of a model based, fundamentally, on

in the control of compliance to another that rests on the principle of responsibility

active, which requires a prior assessment by the person in charge or by the person in charge of the

treatment of the risk that could be generated by the treatment of personal data.

personnel to, based on said assessment, adopt the appropriate measures".

It requires a conscious, committed, active and diligent attitude. consciousness

assumes knowledge of your organization by the data controller and

of how it is affected by data protection and the risks inherent to the

personal data processing; Commitment involves the will to comply and the

be truly responsible for the implementation of protection policies

of data in the organization; the active attitude is related to proactivity,

effectiveness, efficiency and operability; and diligence is the care, zeal and dedication

tion put into compliance.

Based on the foregoing, it can be affirmed that, from the instruction of the procedure, as

as inferred from the Proven Facts and considering the context of article 24 of the

RGPD in relation to SIMYO, it was verified, among others, the implementation of a mo-

the most effective way to avoid 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.

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. For all the above, we focus the facts on the infraction

tion derived from article 5.1.f) of the RGPD.

However, it has been proven that the measures implemented by SIMYO were insufficient.

and not only because they have been overcome and the transfer of personal data

nals to a third party.

In a non-exhaustive manner and by way of example, we will note that the policy of

security that SIMYO applied, allowed (...).

Cases have also been detected in which (...) have occurred. In this sense,

the SIM duplication procedure should include assigning the SIM to the customer

or line when it is sent or delivered, so that during activation

A SIM can only be activated when it has actually been delivered to the customer in

question.

Likewise, in the Seventh Proven Fact, we have outlined the inconsistencies detected

gaps between the security policy and the documented instructions. In this sense,

to improve compliance with security policies the instructions that are

transferred must be clear and up-to-date (without the different time frames in

those that are issued the different documents condition their readjustment).

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.

He adduces the confusion in the Antecedents and in the Proven Facts, on the two su-

posts analyzed. In this sense, we recognize that in the Background of the Pro-

Resolution setting, where it says:

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

December 2019, files a claim with the AEPD against

ORANGE ESPAÑA VIRTUAL, S.L. with NIF B85057974 (hereinafter, SIMYO),

for the following reasons: (...)

SECOND: A.A.A., (hereinafter, the claimant party two), on the 6th of no-

November 2019, file a claim with the Post Office of

Torrehermosa Farm, which is registered with the AEPD on November 13.

2019, directed against SIMYO, for the following reasons: (...)

Should say:

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

December 2019, files a claim with the AEPD against

ORANGE ESPAÑA VIRTUAL, S.L. with NIF B85057974 (hereinafter, SIMYO),

for the following reasons: (...)

SECOND: C.C.C., (hereinafter, the claimant party two), on the 6th of no-

November 2019, file a claim with the Post Office of

Torrehermosa Farm, which is registered with the AEPD on November 13.

2019, directed against SIMYO, for the following reasons: (...)

However, beyond these two material errors that affect six words

(Article 109.2 LPACAP), rectified in this Resolution, cannot adduce SIMYO,

that defenselessness has been generated. This is recognized by the STC 86/1997, of 22 Apr., FJ

1, «the defenselessness must be material, and not merely formal, which implies that this

formal defect has caused real and effective damage to the defendant in his

defense possibilities (STC 43/1989, 101/1990, 6/1992 and 105/1995, among others)”,

since it made allegations both to the Initiation Agreement and to the Proposed Resolution-

tion.

In no way does this confusion affect the Proven Facts that identify the claimants.

keep the respective files:

- no. reference E/10534/2019, claimant party one.

- no. reference E/00220/2020, claimant party two.

Or the information related to the email: ***EMAIL.1, once the name has been corrected,

exposed me.

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 happen, especially when it is duly motivated. At the beginning of

this FD we already indicated that the Agency's actions were aimed at analyzing

the procedures applied to SIM card change requests. SIM card

It constitutes the physical support through which personal data is accessed.

end of the affected person. If their disposal and control are not guaranteed, access to the

personal data of the owner, as well as the possible use or uses by third parties, becomes

in 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;

SIMYO, is responsible for the data processing referred to in the background

exposed, since according to the definition of article 4.7 of the RGPD it is the one 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 Proven Facts.

two, 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, it is required that the holders of all

All SIM cards, whether prepaid or contract, are duly identified.

two and registered. This is important because subscriber identification will be important.

dispensable to register the SIM card, which will mean that when obtaining

a duplicate of this the person who requests it must also identify himself and that

your identity coincides with that of the owner.

SIMYO adduces a series of nuances regarding the data subject to treatment.

The treatment activity questioned has been the request and action management model.

Activation of duplicate SIM cards that -currently- lend through (...), not the

Processing carried out by third parties or other entities, such as financial,

that invokes

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 provider

dor a personal data in the sense of article 4, point 1, of Regulation 2016/679,

when he has legal means that allow him to identify the interested person.

resada thanks to the additional information available to the internet access provider.

internet 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

inextricably linked to natural persons. There is usually an iden-

direct and indirect certifiability. First of all, the telecommunications operators

cations that provide access to the mobile Internet and through the GSM network

They usually have a record with the name, address and bank details.

numbers for each customer, along with various unique device numbers, such as the

IMEI and IMSI. (…)”

In fact, the clause “2.1.2. SIM card” of the “General conditions of the services

SIMYO Services”, provides: The SIM Card is a card that allows you to identify the service

service subscribed by the Client and the contracted line to be able to provide the Mobile Service.

The Customer must insert the SIM Card into their mobile device.

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 exposed by SIMYO:

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

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-

mentioned 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 SIMYO 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.

SIMYO reasons that there are other corrective mechanisms, however, he insists

the latter, 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).

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, SIMYO's participation in the GT (via ORANGE) does not change

the responsibility now imputed to him. Therefore, due to the fact that

has participated in a WG whose objective is to deal with such a criminal activity

("SIM Swapping"), does not prevent that once an infraction has been

tion, should be sanctioned.

2. FIRST ALLEGATION.- 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 SIMYO's opinion, no personal information has been accessed other than the

that the supplanters have contributed. The Agency disagrees with this argument,

because, as stated by SIMYO 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. Also, let us remember that recovery was allowed

of the password to access the Personal Area, which allowed the fraudulent activation

card lens through the “SIM change/duplicate” option, supplanting the

identity of the legitimate owner.

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

users of this sector (article 41 LGTEL) is also bound by the “obligations

regulations of a public nature" applicable to the electronic communications sector (Tí-

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 for them to 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, SIMYO, in the document cataloged as (...) (SIM Swapping)” says:

(…)

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, it will be necessary to obtain the duplicate of the SIM card owned by

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 are outside the responsibility imputed to SIMYO.

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 are not

object of analysis in this file.

3. SECOND ALLEGATION.- UNFOUNDED GENERALIZATION OF CONSE-

NEGATIVE ACCOUNTS ASSOCIATED WITH THE ISSUANCE OF THE DUPLICATE.

SIMYO reiterates the allegations made previously, in respect of which the

AEPD reproduces what it already determined in the Resolution Proposal.

We have already indicated that we upheld the allegation that the access

The duplicate does not provide direct access to the contacts stored on the card.

ta original SIM, since, being a physical device, all the

data it contains and you will not be able to recover the lost contacts on the card

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.

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 it, who requests the duplicate, should
meet strict requirements. It is not that the information to which
refers 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."

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

SIMYO, so there can be no talk of non-compliance with protection measures,

point out that access to the duplicate of a SIM card that makes its holder identifiable

holder, 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.

SIMYO considers that its protocols are adequate and communicates a percentage of

minimal risk of ***NUMBER.4% of cases.

As we have indicated before, the Agency has focused not only on the

fact that third parties have overcome the security measures implemented by

SIMYO, 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.

SIMYO invokes a breach of the principle of strict liability 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

investigated the “fraudulent practices based on the generation of duplicates of

SIM cards without the consent of their legitimate owners in order to access

confidential information for criminal purposes (known as “SIM Swapping”)”

as a consequence of “the news that appeared in the media”, as

as can be deduced 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

find out if there could be a flaw in the privacy protection model.

It is not true, as SIMYO pretends to make it appear, that the

circumstances -exclusively- of two specific cases, since, aside from

these claims, has been directed to analyze whether the technical measures and

organizational arrangements adopted by SIMYO for the issuance of duplicate cards

SIM to the holders of the telephone lines were the appropriate ones to ensure the

mitigation of potential risks to the fundamental rights and freedoms of

line holders.

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 SIMYO, which has also recognized its revision, improvement and reinforcement, and

a total of ***NUMBER.1 cases (together with the ORANGE brand) during the year 2019.

In addition, it must be taken into account that the seriousness of the proven facts is

reflected in the social alarm generated by the performance of these practices

fraudulent, without determining the number of claims filed.

SIMYO alleges that the overcoming of the 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

verify that, despite having access to personal data by

an unauthorized third party, a sufficient level of diligence had been displayed and

adequate even if the security measures implemented had been overcome.

In said file, the circumstances were different. It was a third party

was making a series of queries and requests about the owner's line,

because it had the personal information of the claimant through the link

that had brought them together. 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

cyber criminal. For its part, the operator implemented not only measures to avoid

that such situations occur in general, but also for the case

concrete. And, finally, that claim was closed in application of the principle of

presumption of innocence, which prevents imputing an administrative infraction when

no evidence or indication has been obtained from which the existence of

infringement. The case being resolved now is different, in which -in addition to

the two claims -, a series of cases reported by the

SIMYO itself, in which access to ***NUMBER.1 has materialized

improperly duplicated SIM cards (along with the ORANGE brand), such as

consequence of lacking the appropriate security measures to avoid it.

SIMYO also cites file E/00536/2016 in which the identity is supplanted

to modify the claimant's data on the ORANGE intranet. And he 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: “There have been no supporting evidence that

allow attributing to ORANGE a violation of the regulations regarding

data protection, to the extent that it acted diligently” and,

consequently, it archives the procedure”.

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 that Orange had to identify the person who carried out

the request of the terminals had been enough to understand that there was

acted with reasonable diligence. In this sense, it was considered that ORANGE

used reasonable diligence since -precisely-, it adopted the measures

necessary 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, canceled the requested orders.

However, we are facing different assumptions, given that in the file

E/00536/2016 only the fraud is specified in the execution of orders

fraudulent mobile terminals, while this procedure is about

provide a duplicate of a SIM card (personal data) to someone who is not its owner, which

which leads, as has been repeatedly explained, to a loss of control of

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

record at no time states that the measures taken by ORANGE

were suitable. What it affirms is that: “the lack of evidence has been verified

reasons of the existence of an infraction (...), not proceeding, consequently,

the opening of a sanctioning procedure”. And this under the principle of

presumption of innocence, according to which an infraction cannot be imputed

administrative when no evidence or indications have been obtained of which

results in the existence of an infringement. The fact of affirming that they have not

verified evidence of infringement by ORANGE is very different from affirming

that the measures taken by ORANGE were adequate, which is not the case in

this file.

SIMYO 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 lines

contracted telephone companies using your personal data without consent, for

understand that the claim in question had been addressed, by blocking ORANGE

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

to the detriment that the Agency, applying the investigative and corrective powers

that it holds, can carry out subsequent actions related to the treatment of

information referred to in the claim. This is, without prejudice to which, this Agency

You can investigate the procedure followed in general for this type of

facts. Therefore, even if in that specific case the

claim in question, this does not prevent the Agency from examining the

security measures that SIMYO has in order to prevent a third party from

hire telephone lines in your name without your consent.

For its part, SIMYO also mentions file E/05272/2018, in which

Various workers spread images of clients suspected of having

stolen objects via WhatsApp and, there being no indication that the entity had

breached its obligations in compliance with the principles of integrity and

confidentiality, proceeded to agree to file the proceedings.

In this regard, this Agency wishes to point out that the factual assumption is

considerably different from the one analyzed in this sanctioning procedure. And that,

the fact that in said file no reasonable evidence had been obtained

of the existence of a security breach in the treatment carried out by the

responsible for treatment with respect to the data of its clients, this does not preclude

that in this sanctioning procedure it had been verified that SIMYO had

facilitated access to some SIM card duplicates requested in a

fraudulent, as a result of having security measures that do not

are suitable for this purpose.

SIMYO also mentions file E/07129/2014, in which the AEPD files

the procedure based on, not being possible to determine the identity of the

offender, the principle of presumption of innocence prevents imputing a violation

administrative when the existence of a

supporting evidence 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 it is not

had obtained evidence or indications from which the existence of

infraction, an issue that does occur in the analyzed case.

SIMYO cites file E/08205/2019, in which there was a breach of

security, in which names, surnames and other personal data of

customers, reaching more than 1,300,000 affected. The Agency considered that the

defendant entity had the necessary technical and organizational measures

to deal with a breach such as the one that occurred and that it adopted the additional measures

necessary 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 to

through the deep web. And that during the investigation carried out, it was found that

the security measures that the data controller had were

adequate to deal with an incident of these characteristics and that there

reacted diligently in order to notify, communicate and minimize the

impact and implement reasonable measures to prevent a recurrence

a similar incident in the future. However, in addition to the factual assumption

is considerably different from the assumption analyzed here, the fact that in said

file, it would have been appreciated that the data controller had the

appropriate security measures, this does not prevent this procedure from

sanctioning party it has been proven that SIMYO facilitated access to duplicates of

SIM card, without ensuring the identity of its holders.

Lastly, SIMYO 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

claimed had security measures in place that were, in principle,

adequate. Thus, it is considered that the actions of the defendant as responsible for the

treatment is in accordance with data protection regulations, archiving,

consequently, 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

The facts show that as soon as the attack was detected and confirmed by the

entity, a series of security measures were immediately adopted

in order to minimize the risks and extreme the difficulties for the

access and extraction of information. As stated above,

in addition to the assumption of fact being considerably different from the assumption of

analyzed fraud, the fact that in said file it had been appreciated that the

data controller had the appropriate security measures in place to

the specific case, it does not prevent that in this procedure it has been verified that

SIMYO had access routes to obtain the duplicates (kiosks

dispensers or telephone activations) that favored impersonations of

identity.

SIMYO argues that the fact of allowing in certain

situations the use of non-face-to-face channels with no lack of diligence, in

so much 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 measures of

stringent security measures on 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

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 ***NUMBER.7 euros, does not exempt the operator from its obligations

with those in charge of treatment.

From SIMYO's statements the conclusion seems to be drawn that he has no

no power of action to prevent these frauds or impersonations, since

attributes all responsibility to intervening third parties (managers or

impersonators). 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

treatment. 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. (…)

SIMYO must assess the (real) possibility of such a situation occurring and it is his

obligation to implement measures to avoid this type of situation or, at least, the

quickly detect. Consider all these alleged deviations from the

protocols established by SIMYO as mere specific events before which

no additional actions are carried out to avoid them, it means not acting with the

due diligence and it is for this reason that SIMYO is considered to have infringed the

obligation to ensure the confidentiality of personal data in the event

analyzed here, as a consequence of lacking, precisely, the measures of

adequate security for this purpose.

Nor has this Agency required the "full monitoring of employees", as

as SIMYO states. It simply requires that some measures of

security according to the risk that exists that the agents do not comply with the

measures provided by SIMYO, among others.

SIMYO affirms that (…). However, the mere fact of (...), if later they are not going to

use those (...) to check the effective activity of users and adopt

new measures, cannot be considered as a sufficient and adequate measure to

the stated purposes. Let us recall that in the case of complaining party two,

prior to the delivery of the duplicate (08/23/2019 17:48:43), the

affected sent that same day (08/23/2019) at 17:02 an email

addressed to "soporte@simyo.es" warning that someone had called him from

a hidden number posing as a SIMYO operator to obtain their

personal data, and still, I can't prevent the forwarding.

Finally, it must be remembered that this is not the only security measure that

analyzes nor the only one that could be used to ensure the confidentiality of the

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, the infringement is considered proven. For all of the above, the infraction that

imputed is the one provided for in article 5.1.f) of the RGPD.

Lastly, SIMYO indicates that "the nature of the fundamental right of the right to

data protection does not eliminate the need to examine the diligence displayed

by SIMYO, nor the consideration of the tiny percentage of incidents that have been

produced 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.

First of all, the AEPD also performs functions related to the

digital rights (articles 89 to 94 of the LOPDGDD).

Secondly, the exercise of sanctioning power has been carried out

prior administrative procedure, accompanied by due guarantees, and has

led to determine the Facts, prove guilt and grade the response

administrative. This graduation has not been made outside the circumstances

concurrent, but as a manifestation and requirement of the principle of

transparency (article 3.1.c) LRJSP) and right to good administration

(Article 41 of the Charter of Fundamental Rights of the EU), the facts

have treated impartially and equitably, motivating at all times the

final decision.

Therefore, the Agency has limited itself to analyzing the circumstances of the case

in order to identify the existence of indications or evidence (or not) of

infringement within its jurisdiction. And as a consequence, it has considered

proven that SIMYO has violated one of the principles relating to the treatment

(article 5.1.f) RGPD).

5. FOURTH ARGUMENT. – SIMYO'S DILIGENT PERFORMANCE.

He invokes a total defenselessness, because despite the fact that he has managed to prove the

fulfillment of his duty of diligence and being recognized, is subject to a

sanction for an unspecified reason.

The Agency has scrupulously respected the procedure, allowing SIMYO

the exercise of their right to effective protection, since in this procedure

the principles of bilateralism, contradiction and equality of arms have been respected

as required by the reiterated doctrine of the Constitutional Court on the right

to effective judicial protection that (Valga for all Sentence 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 art. 24.1 CE, guarantees the right to access the process and resources legally established in conditions of being able to be heard and exercise the defense of the rights and legitimate interests in a procedure in which the principles of bilaterality, contradiction and equality of procedural weapons, (...) (SSTC 167/1992, from 26 Oct; 103/1993, of March 22; 316/1993, of Oct. 25; 317/1993, of Oct. 25; 334/1993, of Nov. 15; 108/1994, of Apr. 11; 186/1997, of Nov. 10; 153/2001, of 2 Jul.; 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 supposed a real and effective damage to the defendant in his defense possibilities (STC 43/1989, 101/1990, 6/1992 and 105/1995, among others)"; in this sense, SIMYO, in at all times he has had knowledge of the facts imputed to him, the possible infractions of which the facts are constitutive, has been able to allege as to its law has deemed 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 sanctioning procedure and, that 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. For this reason, we reject the allegation made.

Likewise, far from SIMYO'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 sanctioning procedure and more specifically SIMYO's right to defense.

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.

Lack of diligence in implementing security measures at source

adequate constitutes the element of culpability.

Regarding the responsibility of SIMYO, it should be noted that, in general

SIMYO treats the data of its clients under the provisions of article 6.1 b)

of the RGPD, as it is considered a necessary treatment for the execution of a

contract in which the interested party is a party or for the application at the request of the latter of

pre-contractual measures. In other cases, it bases the legality of the treatment on

the bases provided for in article 6.1.a), c) and f) of the RGPD. In this sense, SIMI

has a network of commercials, points of sale and distributors approved to

through a distribution contract to offer SIMYO services. Among

these services offered from their points of sale, is the realization of

SIM card duplicates corresponding to a mobile phone line.

Let us remember that clients -individuals or legal entities- sign contracts with

SIMYO for the provision of certain services that are subject to certain

privacy clauses contained in the Privacy Annex as provided by the

clause 13.1 of the “General Conditions of SIMYO Services”.

Just as SIMYO requires customers to comply with the obligations

specified in the contracts signed with the operator, from this, the

compliance with the obligations that in terms of security and confidentiality

compete.

For example, clause 13.3 of the General Conditions of the Services of

SIMYO says:

(vi) In particular, SIMYO undertakes to comply with the following

obligations:

a. Treat personal data, only, to carry out the provision

of the contracted services, adjusting to the instructions that, in each

moment, indicates, in writing, the Client (unless there is a regulation

that requires complementary treatments, in such a case, SIMYO will inform the

Client of that legal requirement prior to treatment, unless such Right

prohibited for important reasons of public interest).

b. Maintain the duty of secrecy regarding personal data to

which you have access, even after the contractual relationship has ended,

as well as to guarantee that the people in their charge have committed themselves

in writing to maintain the confidentiality of the personal data processed.

c. Guarantee the application of appropriate technical and organizational measures,

taking into account the state of the art, the application costs, the

nature, scope, context and purposes of the treatment, as well as

risks of varying likelihood and severity to rights and freedoms

of natural persons, to guarantee a level of security appropriate to the

risk, which in your case includes, among others:

(i) pseudonymization and encryption of personal data,

(ii) the permanent confidentiality, integrity, availability and resilience

treatment systems and services

(iii) the ability to restore availability and access to data

quickly in the event of a physical or technical incident

(iv) a process of regular verification, evaluation and assessment of the

effectiveness of technical and organizational measures to ensure safety

of the treatment.

d. Keep under your control and custody the personal data you access

for the provision of the Service and not to disclose, transfer, or

communicate them in any other way, not even for their conservation to other

people outside the same and the provision of the service. However, the

Customer may expressly authorize SIMYO in writing to

resort to another Treatment Manager (hereinafter, the "Subcontractor").

SIMYO will inform the Customer in the same way of any planned change in

the incorporation or substitution of the Subcontractors, thus giving the Client the

opportunity to oppose such changes.

Regarding due diligence, we acknowledge that SIMYO has acted

subsequently diligently in order to minimize the impact to possible

affected by implementing new security measures to avoid the repetition of

similar incidents 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 administratively, as well as, when a Law

recognize 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

attributable to human behavior. So, in the case of violations

committed by legal persons, although the element of

guilt, this is necessarily applied differently from how it is done

with respect to natural 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 sense, but not the ability to break the rules to which they are

subdued.

Capacity for infringement and, therefore, direct blame that derives from the good

protected by the norm that is violated and the need for said

protection is really effective and for the risk that, consequently, it must assume

the legal entity 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,

partially transcribed in the SSTS of October 9, 2009, Rec 5285/2005, and of

October 23, 2010, Rec 1067/2006, that "although the culpability of the conduct

must also be 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 normative aspect, that the diligence that was required by whoever alleges its non-existence; not enough, in short, for exculpation in the face of a typically unlawful behavior the invocation of the absence of fault".

In the cases of complaining parties one and two, the (...) was provided, as It is stated in the Third and Fourth Proven Facts of this Resolution.

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 It is necessary for a third party to “impersonate the identity” of the owner of the data before the financial entity. 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 basis legal, 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 operators is essential to avoid this type of scams and violations of the GDPR. Diligence that translates into the establishment of adequate measures to guarantee that the 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 a adequate security in the processing of personal data, security that is not has guaranteed in accordance with the Proven Facts. And this is so, because provided duplicate SIM cards to third parties other than legitimate holders of mobile lines, after overcoming by these of the policy of existing security, which shows a breach of the principle of confidentiality.

Illegality is the quality that has a conduct previously typical of

violate the legal system and the purposes it pursues. In this way, for

be liable to sanction it is not enough that the conduct fits the description

contained in the type, but with it the objectives are being violated

prosecuted by law. In this regard, the conduct will be unlawful if the

legal right protected by the precept violated.

In this case, the legislation on the protection of personal data pursues the

purpose that those responsible and in charge of the data carry out a treatment

of these having security measures that prevent the illicit use or

fraudulent of them. And this legal right has been injured in the facts

object of this procedure.

Consequently, the allegations made are dismissed, including the lack

of guilt.

6. FIFTH ARGUMENT. – LACK OF PROPORTIONALITY OF THE PENALTY

PROPOSAL.

Regarding the breach of the principle of proportionality, the RGPD provides

expressly the possibility of graduation, through the provision of fines

susceptible to modulation, in response to a series of circumstances of each

individual case. Although, this aspect will be analyzed in the Seventh FD.

SIMYO 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, 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

must be sanctioned with a fine in view of the serious circumstances

concurrent individuals. Said fine must meet the characteristics imposed by

Article 83.1 of the RGPD, that is, it must be individualized and effective,

proportionate and dissuasive.

The fine must be dissuasive, so that the offending conduct is not

repeat 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, in pointing out in the

section 23 of said judgment that the dissuasive factor is valued taking

into consideration a multitude of elements and not just the situation

particular to the company in question, he was referring to points 53 to 55 of

the conclusions presented in that case by the Advocate General

Geelhoed, who had pointed out, in essence, that the multiplier coefficient

of a deterrent nature may have as its object not only a 'deterrent

general", defined as an action to discourage all

companies, in general, that commit the infringement in question, but

also a "specific deterrence", consisting of dissuading the defendant

so that you don't break the rules again in the future. For the

Therefore, the Court of Justice only confirmed, in that judgment, that the

Commission was not required to limit its assessment to factors

related solely to the particular situation of the company in

question."

“102. According to settled case law, the objective of the multiplier factor

dissuasive and the consideration, in this context, of the size and the

global resources of the company in question lies in the desired impact

on the aforementioned company, since the sanction should not be insignificant,

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

pecuniary sanctions must provide that the commission of offenses typified

is not more beneficial to the offender than compliance with the rules

violated”.

The fine must generate a dissuasive effect with respect to non-compliance and violation of data protection regulations and never be more beneficial to the offender than compliance with the rule violated.

On the other hand, SIMYO 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 an eventual damage to the person responsible for the treatment is not considered as a mitigating factor by the regulations of data protection and this is observed from the simple reading of articles 83.2 of the RGPD and 76.2 of the LOPDGDD, we remind you again that the purpose of this procedure focuses on the absence of security guarantees that has allowed the unauthorized or illicit access of third parties to the personal data of the interested.

The possible damages that it indicates that it suffers, since it has had to carry out "internal investigations, make compensation to the complainants and reassess procedures and protocols", are caused by their own negligence, since that, if adequate security measures were in place, such access by third parties would not have occurred and the subsequent crime would not have materialized.

All those damages related to internal investigations and reevaluation of procedures and protocols do not cease to be obligations of the proactive responsibility imposed from risk management, among others many duties, the maintenance, updating and control and auditing of the data protection policies in an organization.

The compensations to the claimants also derive from the assignment of the personal data of those affected to third parties -enabling the subsequent commission of crimes- which constitutes a fault also attributable to SIMYO, consequence of the

violation 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, SIMYO's participation in the GT does not modify the responsibility

now he is charged once the infraction is verified.

FOURTH.- PRINCIPLES RELATED TO TREATMENT.

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 infraction imputed to SIMYO, but they offer a perspective

of possible risks derived from the treatment in question. Risk management assumed

There is a reflection exercise that must be carried out before carrying out an activity

of personal data processing. Its objective is to identify and be able to anticipate

to the possible adverse effects, or unforeseen, that the treatment could have on

the interested. It must allow the person in charge to make the necessary decisions and actions.

necessary to ensure that the treatment meets the requirements of the RGPD and the LO-

PDGDD, guaranteeing and being able to demonstrate the protection of the rights of the inte-

resados.

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 SIMYO herself, they would have failed to comply with any of the instructions
tions 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 data controller (SIMYO as has been proven
in this file).

SIMYO cannot shirk its responsibility for the safety

treatment, hiding behind the breaches of those involved in the management

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 SIMYO, and inevitably, the resulting

ted.

Regarding the special relevance of the SIM card, we refer to the modern graduation

tivated in the Seventh FD.

Finally, regarding the deployment of security measures, there is no doubt that SI-

MYO has reviewed the protocols to prevent identity theft in these

processes; has transferred the information to those involved in the processing; has introduced

do improvements after knowing certain vulnerabilities; including penalties for their

breach. However, we do not share the fact that it has been carried out

an appropriate and adequate deployment of security measures, in the terms of art.

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.- SECURITY 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 supplanting persons, having
facilitated, by SIMYO, in addition, (...). Consequently, their powers of
disposal and control over your personal data, which constitute part of the content
of the fundamental right to data protection as stated by the Constitutional Court

in Judgment 292/2000, of November 30, 2000 (FJ 7). By way of

that, by obtaining a duplicate of the SIM card, it is possible under certain circumstances

circumstances, access to contacts or applications and services that have

as a password recovery procedure, sending an SMS with a code to

be able to change passwords. In short, they may supplant the identity of the

affected, being able to access and control, for example: email accounts

co; bank accounts; applications like WhatsApp; social networks, such as Facebook

or Twitter, and a long etc. In short, once the password has been changed

by impersonators lose control of their accounts, applications and services.

cios, 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 SIMYO duplicates of the SIM card to third parties

people who are not the legitimate owners of the mobile lines and even modify the

personal data -email-, after overcoming by the supplanted people-

of the security policies implemented by the operator, which shows an in-

compliance with the duty to protect customer information.

This unauthorized access to the SIM card is decisive for the actions

developed by the supplanting people whose purpose is to obtain

have an economic benefit (there are calls to financial entities and the

of banking operations in both claims), since the impersonator takes advantage

the length 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

for which SIMYO have a legal duty to ensure your 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 the

information technology offers both to collect and to communicate personal data or

the undoubted risks that this can entail, given that a person can

ignore not only what data that concerns you that is 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 right

fundamental to privacy (art. 18.1 CE) does not provide by itself a protection

sufficient 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

informatics and entrusted to the legislator the guarantee of both certain rights

fundamental as the full exercise of the rights of the person. That is,

incorporating a guarantee institute "as a form of response to a new

form of 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 your 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, they were dissipated by highlighting that
these rights, in view of their content, did not offer sufficient guarantees
against the threats that the use of informatics could entail for the
protection of privacy. So the constituent wanted to guarantee
through the current art. 18.4 CE not only a specific scope of protection but
also more suitable than the one that could offer, by themselves, the rights
fundamentals 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 right or freedom
fundamental, the right to liberty against potential aggressions against
dignity and freedom of the person arising from an illegitimate use of
mechanized data processing, what the Constitution calls 'informatics'",
what 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 of the private life of the person and his reputation today have a
positive dimension that exceeds the scope of the fundamental right to

privacy (art. 18.1 CE), and that translates into a right of control over the

personal data. The so-called "computer freedom" is like this

right to control the use of the same data inserted in a program

(habeas data) and includes, among other aspects, the opposition of the

citizen to certain personal data being used for purposes

other than the legitimate one that justified obtaining it (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

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. In the end, the right to privacy allows certain data of a person to be excluded from the knowledge of others, for this reason, and this Court has said so (SSTC 134/1999, of July 15, FJ 5; 144/1999, FJ 8; 98/2000, of April 10, FJ 5; 115/2000, of May 10, FJ 4), that is, the power to protect his life deprived of unwanted publicity. The right to data protection guarantees individuals a power of disposition over these data. Is guarantee imposes on the public powers the prohibition that they become sources of that information without due guarantees; and also the duty of prevent risks that may arise from improper access or disclosure of said information. But that power of disposal over the data itself nothing is worth if the affected party does not know what data is being owned by third parties, who owns them, and for what purpose.

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 sometimes defined in broader terms as sphere of the goods of the personality that belong to the realm of life privacy, inextricably linked to respect for personal dignity

(STC 170/1987, of October 30, FJ 4), as the right to honor, cited

expressly in art. 18.4 CE, and also, in a very broad expression of the
art itself 18.4 CE, to the full exercise of the rights of the person. The right
fundamental to data protection extends the constitutional guarantee to
Those of these data that are relevant to or have an impact on the
exercise of any rights of the person, whether or not they are
constitutional and whether or not related to honor, ideology, privacy
personal and family property to any other constitutionally protected property.
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 may affect their rights, whether fundamental or not, because their
object is not only individual intimacy, for this is the protection that the
art. 18.1 CE grants, but personal data. Therefore,
also reaches those public personal data, which by the fact of
be, if they are accessible to the knowledge of anyone, they do not escape the power of
disposition of the affected party because this is guaranteed by his right to the protection of
data. Also for this reason, the fact that the data is of a personal nature does not mean
that only those related to the private or intimate life of the person have protection.
person, but the protected data are all those that identify or
allow the identification of the person, being able to serve for the preparation of
their ideological, racial, sexual, economic or any other profile, 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
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 July, 144/1999, of July 22, and 115/2000, of May 10), the right to data protection attributes to its holder a bundle of powers consisting of various legal powers whose exercise imposes legal duties on third parties, that are not contained in the fundamental right to privacy, and that serve the capital function performed by this fundamental right: to guarantee the person a power of control over their personal data, which is only possible and effective imposing on third parties the aforementioned duties to do. Namely: the right to require prior consent for the collection and use of personal data, the right to know and be informed about the destination and use of these data and the right to access, rectify and cancel said data. In definitively, 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 disposal and control over the personal data that empowers the person to decide which of these data provide to a third party, be it the State or an individual, or what this

third party collect, and that also allows the individual to know who owns those
personal data and for what, being able to oppose that possession or use. These
powers of disposal and control over personal data, which constitute
part of the content of the fundamental right to data protection is
legally specified in the power to consent to the collection, obtaining and
access to personal data, their subsequent storage and treatment,
as well as its possible use or uses, by a third party, be it the State or an individual.
And that right to consent to the knowledge and treatment, computerized or not, of
personal data, requires as essential complements, for a
On the other hand, the power to know at all times who has that data
personal information and to what use it is subjecting them, and, on the other hand, the power to oppose
to that possession and uses.
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
themselves. And they are indispensable to make this content effective
recognition of the right to be informed of who owns your data
and for what purpose, and the right to object to such possession and use
requiring the appropriate party to put an end to the possession and use of the
data. In other words, requiring the owner of the file to inform him of what data
owns on his person, accessing their appropriate records and seats, and
what fate they have had, which also reaches potential assignees; and, in his
case, require him to rectify or cancel them.” (the underline of all
the paragraphs is ours)
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) Submission by the person in charge or in charge, on a voluntary basis,

voluntary, to mechanisms of alternative resolution of conflicts, 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) GDPR:

□

The nature, seriousness and duration of the offence, taking into account

the nature, scope or purpose of the processing operation that

concerned as well as the number of stakeholders affected and the level of

damages that they have suffered:

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 online payments

ne to be 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 SIMYO alleges, the seriousness of the infringement focuses on

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 in the actions or omissions of SIMYO that have made possible

do unauthorized or illicit access to personal data of its customers

to third parties due to the absence of appropriate security guarantees,

which has been duly proven.

In all likelihood, if SIMYO had had safety measures in place,

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, but yes to your personal data, as it is put in

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.

Regarding the level of damages suffered, it is considered high.

He argues that it is not feasible to try to hold SIMYO responsible for

situations related to the use of duplicate cards that derive

of information security incidents with which SIMYO does not have

no relationship.

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.

SIMYO is not responsible for customer identification policies

established by banks. However, it is also true

to, that if SIMYO ensured the identification and delivery procedure

of the duplicate SIM card, it could not even activate the system of

Verification of banking entities. The scammer behind con-

follow the activation of the new SIM, it takes control of the phone line.

thus being able to then carry out fraudulent banking operations.

slow accessing the SMS that banking entities send to their

clients as confirmation of the operations they execute. This is-

sequence of facts 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. Concrete-

mind in the case of complaining party one, the activation of the duplicate

occurs at 9:15 p.m. on August 14, 2019 and at 9:35 p.m.

hours of that same day, he receives two informative emails about the contra-

taking out an orange loan and opening a payroll account. In

In the case of complaining party two, the activation of the duplicate occurred

ce at 5:48 p.m. on August 23, 2019. At 6:24 p.m.

that same day, SIMYO proceeds to its effective blocking and deactivation,

however, enough time elapses to effectively usurp

activates the identity of the affected party, modify and control the passwords of the bank

online account with which the legitimate subscriber operates and make a transfer

large amount -30,000 euros-, in his name. Therefore, it constitutes

a general obligation in accordance with data protection regulations,

that SIMYO has technical and organizational measures that are

appropriate for the correct identification of its clients and that guarantee

provide adequate security when safeguarding personal data

of the users.

As has been shown, the damages and losses have been assessed.

prices, at least in relation to those cases in which they have been

laid claims by interested parties.

Regarding the allegations made regarding that there is no impu-

damages or consider them as aggravating, we must

mean that unauthorized or illicit access is a harm in itself

of the personal data of an interested party by a third party when the

fundamental right 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. 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) GDPR:

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

SIMYO, concludes that he was negligent in not ensuring a procedure

that guarantees the protection of the personal data of its clients.

Thus, a socially harmful result is produced that requires

the establishment of additional guarantees in the security policy

implemented so far.

Deny the concurrence of negligent action on the part of SIMYO

would be equivalent to acknowledging that their conduct -by action or omission- has been

diligent. Obviously, we do not share this perspective of the facts,

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 SIMYO'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) GDPR:

Degree of responsibility of the person in charge:

Tall.

He argues that they have adopted many measures and improvements in the procedure.

issue date of the duplicate SIM card.

Responsibility for vulnerabilities in the implanted procedure

ted for the issuance of the SIM corresponds to SIMYO.

Those in charge of the treatment -in its case-, can only treat the damages

cough following the documented instructions of the person in charge.

The personal data that SIMYO collects both for contracting the

service and during its provision are your responsibility and must

be treated in a way that allows the proper development of the relationship

between the parties, guaranteeing at all times the application

tion 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 (“agents, who breached the security policy of SIM-

I and the measures it imposed”).

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

necessary to demonstrate compliance with the obligations established

established in this article, as well as to allow and contribute to the

performance of audits, including inspections, by the responsible

saber or 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.g) GDPR:

C/ Jorge Juan, 6

28001 – Madrid

Categories of personal data affected by the breach:

He argues that the SIM card does not allow identity theft, but rather

that serves only for the reception of the confirmation keys of

banking operations in certain cases.

SIMYO claims that only basic data of the

customers and that the SIM card is not personal data, since

We scam this argument in the Fourth FD.

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, with the purpose of in-

interact and perform operations on your behalf, authenticating through

a username and password previously taken from that user, as well

as with the two-factor authentication when receiving the confirmation SMS.

mation in your own mobile terminal where you will have inserted the SIM card

duplicated.

In this sense, bringing up again the aforementioned SAP of Barcelo-

na no. 390/2019 of May 30.

And therefore, the claim that it be considered as

extenuating.

- Article 76.2.b) LOPDGDD:

Linking the activity of the offender with the performance of

processing of personal data:

The development of the business activity carried out by SIMYO requires

re continuous and large-scale processing of the personal data of

the clients. according to the number of mobile voice lines reported

called in the "NINETEENTH Background", which positions SIMYO

as one of the three largest telecommunications operators

of our country.

It is not that in the event of any infraction committed by the merchant,

will apply this aggravating factor, but that, in the circumstances

individual of the case, its application proceeds.

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.

(…)

- Article 83.2.f) GDPR:

□

Degree of cooperation with the control authority:

Tall.

The Agency considers that SIMYO has cooperated favorably with

research, providing a response to the requirements and training

command part of the GT (through ORANGE), which is valued

positive.

- Article 76.2.c) LOPDGDD:

□

The benefits obtained as a result of the commission of the

infringement.

He claims that he is one more victim of the criminal network.

This Agency does not consider that it has obtained an economic benefit

beyond receiving the price of the cost fixed for the issuance of the du-

SIM card applications.

- Article 76.2.h) LOPDGDD:

Submission to conflict resolution mechanisms.

Various telecommunications operators, including

SIMYO, signed a Protocol with AUTOCONTROL that, without

prejudice to the powers of the AEPD, provides mechanisms

for the private settlement of disputes relating to the protection of

data in the field of contracting and advertising services

electronic communications, dated September 15, 2017.

Protocol whose effective application must be considered as

extenuating.

The allegations made in relation to article 83.2.a), b), d) and g) are rejected.

of the RGPD and article 76.2.b) of the LOPDGDD, in the terms previously stated.

posts.

As has been proven in the instruction of this procedure, the imposition of

the sanction derives from Proven Facts that constitute a very serious infraction

of the GDPR. The facts are imputed to SIMYO as responsible for the treatment of the

issuance of duplicate SIM cards, therefore, should be strongly rejected

the statement made regarding that "you cannot take into consideration assumptions

in fact not examined in the present procedure, where the

derived responsibilities and the treatments and conduct, therefore, said su-

posts cannot be used to harm, in any case, SIMYO, as long as

No infraction or non-compliance has been proven".

Finally, it requests that the fine be replaced by "the adoption of corrective measures
measures contemplated in the aforementioned article 58, consisting of the warning or
treatment to the data controller and the imposition of the obligation to adopt
measures to carry out the treatments “in a certain way and within a certain
specified term”.

This request must also be dismissed. Understanding the corrective system
provided for in the RGPD that SIMYO 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 having assessed the criteria for

graduation of the sanctions whose existence has been proven, the director of the

AEPD, RESOLVES:

FIRST: IMPOSE ORANGE ESPAÑA VIRTUAL, S.L., with NIF B85057974, for

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

classified as very serious for prescription purposes in article 72.1.a) of the LO-

PDGDD, an administrative fine amounting to 70,000'00 euros (seventy thousand euros).

SECOND: NOTIFY this resolution to ORANGE ESPAÑA VIRTUAL, S.L.

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

C/ Jorge Juan, 6

28001 – Madrid

938-26102021

www.aepd.es

sedeagpd.gob.es