File No.: PS/00027/2021

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 ONE CLAIMANT), dated October 3 2019, files a document with the Office of ***EMPRESA.1 in Granada, which is registered with the AEPD on October 8, 2019, through which it files a claim directed against XFERA MÓVILES, S.A. (MOREMOBILE), with NIF A82528548 (hereinafter, XFERA), for the following reasons:

"(…) First. On September 25, 2019 YOIGO generated a duplicate of card of my telephone ***TELEFONO.1 being that this part had not requested and being that my personal data have been illegally transferred, including banking.

Second. The above action is contrary to the regulatory principles of the treatment of personal data provided for in Organic Law 3/2018, of 5 of December, of Protection of Personal Data and guarantee of the rights digital: to this effect there are committed at least, the following violations:

The irregular processing of personal data in violation of the principles of consent and information of article 6, of the Organic Law 3/2018, of December 5.

The intentional breach of the duty of secrecy of article 5 of the same organic standard.

The violation of the basic principles of the treatment according to the forecast of the

letter a) of number 5 of art. 83 of REGULATION (EU) 2016/679 OF THE

EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 27, 2016 on

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

personal information. (…)"

Together with the claim, it provides two complaints filed with the General Directorate of

the National Police in the offices of Granada Centro, denouncing these

facts.

In the first of the complaints with report number XXXX/XX, dated 26

September 2019, states:

"(…) That the person appearing yesterday around 6:30 p.m. realized

that your mobile phone from the Yoigo company and with terminal number

***TELEFONO.1 was out of service, so it was put into

contact Customer Service of said company, which informed him that

possibly it would have had a problem with the SIM card.

--That today he has appeared at his Bankia bank to

make some payments, indicating the employee that in the current account of his

daughter, named B.B.B. with the same address and contact telephone number as the

appearing was with only 5.60 euros.

--That since the complainant was sure that in said account

there was more money, that is why Bankia employees have verified

what unknown person/s have accessed the phone's online banking

mobile phone of the appearing party and they have withdrawn 1300 euros from the card of the

complainant have transferred it to his checking account at the Bankia entity and to

Then they have made a refund of 1000 euros for the

procedure Charge.Pag friends to the person of C.C.C. and a refund of 150

euros from an ATM, for which you cannot provide data.

--That they have tried to make another withdrawal at the ATM although it has been blocked

the operation.

--That the complainant is an authorized person in his daughter's checking account

B.B.B., so through their mobile phone they have accessed the account of

his daughter and have made three immediate transfers for an amount of 2000

euros, 800 euros and 100 euros, the recipient being DDD.

--That all this information has been indicated by the Bankia employee, since

both the complainant and his daughter at no time have had

knowledge of what happened and even fewer have authorized the operations

indicated. (…)"

In the second of the complaints with report number YYYY/YY, dated 26

September 2019, states:

"(…) On the twenty-sixth day of today, the decedent filed a complaint in these

dependencies with number XXXX/XX, in which he gave an account of the extraction

fraudulently in his bank account and in the bank account of his daughter,

(B.B.B.), for the total amount of 4,050 euros, an event that occurred on the date and

right place.

--Appearing again to communicate, that after taking steps

with Yoigo's telephone company, it has been reported that the alleged

authors of the narrated events made a duplicate SIM card, with the

telephone number of the complainant, at the Yoigo office, located in Castellón

de la Plana, avenue of the Virgen del Lidón, number 19, with number of

duplicity: (ICC) ***NUMBER.1.

--The appearing party wishing to state that he understands that the company

Yoigo has provided your personal data, in this case to the person

denounced, as well as, has facilitated a duplication of his telephone card,

reason why he is completely convinced that he has also been the victim of a

criminal offense by said telephone company, by providing your data

freely personal. (…)"

It also provides bank receipts for transactions made

authorized.

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 26, 2019, the claim was transferred to XFE-

RA to proceed with their analysis and provide a response within a month.

XFERA, did not respond to this request, notified on November 26

2019, through the Electronic Notifications and Electronic Address Service

Authorized, according to the certificate that appears in the file.

On said claim fell resolution of ADMISSION TO PROCESS dated 11

February 2020, in the file with no. of reference E/11270/2019.

SECOND: E.E.E. (hereinafter, the TWO CLAIMANT), on the 5th of

November 2019, filed a claim with the AEPD against XFERA,

for the following reasons:

“The company MÁSMÓVIL with CIF A20609459 is claimed, which on the day

07/10/2019 was made without your consent in a mobile store a

duplicate of the SIM card leading this to a bank fraud in the bank (ING)

Therefore, I consider that the MÁSMÓVIL company has violated the protection law

of data.

Therefore, I provide the relevant documentation of the events that occurred.

1) complaint and extension of the complaint.

2) amounts of the stolen

3) email from MÁSMÓVIL stating that a duplicate SIM card was made on the day

07/10/2019 at 4:46 p.m.

4) report to the Ministry of Economy and Business (consumer)

5) claim dismissed by MÁSMÓVIL for the events that occurred

(like they don't want to know anything)

The amounts have been paid (returned) by the ING entity thanks to the

occurred in the extension of the complaint. If it is not by the Mosso d'Escuadra

nº ***NUMBER.2 who contacted me to explain how I was

did the fraud, both ING and MÁSMÓVIL would not have returned the amounts

stolen, (...)

So I claim compensation for violating the data protection law and

the inconveniences and disorders caused to solve all this problem, as well

as well as the pertinent sanctions against the MÁSMÓVIL company (…)”

Together with the claim, it provides two complaints filed with the General Directorate of the National Police in the dependencies of Móstoles, denouncing these facts.

In the first of the complaints with report number RRRRR/RR, dated 11 July 2019, states:

“That the complainant states that he has observed in his account number ***ACCOUNT.1 of the ING entity two charges that he has not made or authorized.

That the movements have been made with the card with the number ***TARJETA.1 which is associated with the account referred to above, being the movements following:

On 07/10/2019, withdrawal at the ATM number ***CAJERO.1, for a value of 1700 euros.

On 07/10/2019, withdrawal at the ATM number ***CAJERO.1, for a value of 2000 euros.

That he has also appeared at the bank in order to collect the bank receipt, which contributes to this instruction and is attached to the presents.

That the deponent states that he has never lost his bank card, stating that have never made purchases in this establishment.”

In the second of the complaints with the report number SSSSS/SS, dated 29 July 2019, states:

“That these are extensions of the attested number RRRRR/RR of these

dependencies.

That the respondent states that he received a call on 07/26/2019 throughout '

this day without specifying the exact time. (…)

That the call was supposedly made by the caporal number ***NUMBER.2 of the

Mossos d'Esquadra, responsible for theft and fraud.(...)

That said interlocutor asked the complainant to confirm ownership

of the telephone number of which he was a subscriber since it appeared after a series of

investigations that he was carrying out on bank card fraud, that the

His appeared on a list of defaulters. (…)

That his interlocutor then asked him to forward the complaint that

filed, in order to include her in the investigations that were being carried out

by his police unit (...)

That in said telephone conversation that police agent assured him that his

mobile phone through the stores of the "MASMÓVIL" company would have been the

place from which at some given moment the duplication of its

card, a fact that in this regard the complainant would remember that days prior to the

materialization of the fraudulent charges on your account and for what you filed with

after denouncing, he realized that for a short time his phone

phone was left without a line and unusable, therefore having to change its SIM card.

(…)”

On December 10, 2020, the claim was transferred to XFERA, to

to proceed with its analysis and respond within a month.

In response to said request, XFERA stated -as its sole argument- the following:

following:

“Unique.- Insufficient information.

The claim received refers to alleged criminal acts consistent

in duplicating a SIM card as a means of carrying out bank fraud and that

would have occurred in "(...)".

Naturally, this type of behavior falls completely outside the activity

own and in no way can be produced from the ordinary performance of the

care and management protocols established in the company.

However, given the seriousness of the facts, an attempt has been made to seek some

information about it, but due to the lack of indications in the claim

received it is not possible to provide any additional information outside of

express the desire for full collaboration in the event that it were possible

Specify more precisely what is requested.

On said claim fell resolution of ADMISSION TO PROCESS dated 23 of

February 2020, in the file with no. of reference E/11591/2019.

Said resolution was subject to a rectification of errors on March 5,

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

6/102

FOURTH: In view of the facts denounced by the 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 services addressed to XFERA, on different dates:

Secure Verification Code Requirement

First

Second

Third

***CSV.1

***CSV.2

***CSV.3

Required date

I lie

01/13/2020

06/18/2020

09/18/2020

Notification date-

tion required

I lie

01/16/2020

06/19/2020

09/18/2020

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.

8. Total number of mobile telephony clients of the entity.

In the second of the requirements, dated June 18, 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) In the case of the YOIGO brand, it is indicated that (...).

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

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

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

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

How should you assess the client's circumstances to access the technical procedure?

lephonic

B) In the cases of the LLAMAYA and LEBARA brands, it is indicated that (...).

A copy of the written procedure is also requested where all the

cases being processed (...), including all assumptions, and a copy of the instructions

specific instructions given to operators with detailed information on how to

the operator assesses that the customer cannot go to a point of sale.

C) In the case of the MÁSMÓVIL brand, confirmation of (…).

D) In your answer brief you allude to the security policy that you must pay.

serve the client in telephone requests. A copy of the security policies is requested.

security of all brands, where the data requested is clearly stated.

so 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.

C2) About the application process (…) of LLAMAYA:

Information is requested on whether it refers to (...).

Information on whether the customer can set a delivery address other than the one

usual, as appears from the information provided.

For all brands, in the procedures (...), information is requested on whether it is

possible to change the delivery address of the SIM and under what circumstances.

D2) Checks that are carried out in the home delivery of the SIM card

for recipient identification. Copy of the contractual documentation with

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

identity checks to be carried out by the delivery person.

POINT 2

List of 20 cases of SIM duplicates denounced/claimed as su-

planting identity or fraudulent by customers. The list will include the du-

SIM replicas requested from January 1, 2020, that is, all re-

calls that happened from January 1, from the first, consecutive

up to 20.

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

POINT 3

About cases presented before this Agency that are summarized in the table:

EXPE-

Ref.

TOOTH

E/11270/2019

AND/

Y

1422/2020

E/11591/2019

DATE

FACTS

09/25/201

9

07/10/201

9

FACTS

CUSTOMER DATA

SIM Duplicate

In YOIGO office

SIM Duplicate

MÁSMÓ Office-

VILE

-

-

-

-

-

-

A.A.A.

DNI ***NIF.1

phone

***PHONE.2

E.E.E.

DNI ***NIF.2

phone

***PHONE.3

It is requested:

A) Copies of the DNI collected in the SIM duplicate request. In case of

that there is no copy collected, a reflection that is recorded in the application systems and

verification of the applicant's identity by showing their ID.

B) Information on whether there is a requirement for the delivery that the city

where the SIM is requested is the customer's city of residence. Information on-

Ask if there is any additional control in case of different cities.

C) Actions undertaken by XFERA in each case, including accreditation do-

detail of the following aspects:

~

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

future phishing attempts.

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

with the point of sale.

~

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

resolution of your case.

In the third and last of the requirements, dated September 18, 2020,

requested the following information:

POINT 1

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

listed in the previous answer:

DATE

05/01/2020

C/ Jorge Juan, 6

28001 – Madrid

MSISDN

***PHONE.4

BRAND

MoreMobile

CHANNEL

Telephone

www.aepd.es

sedeagpd.gob.es

01/14/2020

01/15/2020

01/20/2020

01/25/2020

01/27/2020

01/27/2020

01/28/2020

02/04/2020

02/25/2020

02/27/2020

02/29/2020

03/03/2020

05/03/2020

05/03/2020

03/11/2020

03/13/2020

04/03/2020

04/04/2020

04/08/2020

04/12/2020

A. It is requested, in the cases of (...):

***PHONE.5

***PHONE.6

***PHONE.7

***PHONE.8

***PHONE.9

***PHONE.10

***PHONE.11

***PHONE.12

***PHONE.13

***PHONE.14

***PHONE.15

***PHONE.15

***PHONE.16

***PHONE.12

***PHONE.17

***PHONE.18

***PHONE.19

***PHONE.20

***PHONE.21

***PHONE.22

Yoigo

MoreMobile

MoreMobile

Yoigo

MoreMobile

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

MoreMobile

MoreMobile

Yoigo

Yoigo

Store

Telephone

Telephone

Telephone

Telephone

Store

Store

Telephone

Telephone

Telephone

Telephone

Telephone

Telephone

Telephone

Store

Telephone

Telephone

Telephone

Store

Telephone

- Copy of the DNI or identification documents provided by the applicants.

before the SIM change.

- For YOIGO clients, a copy of the document signed by the applicant.

much for the new SIM.

B. For the cases of (...):

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

exceeds the security policy.

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

SIM activation exceeds the security policy.

- Detail of the circumstances that concurred to access the

processing of the telephone request.

POINT 2

Regarding the case ref E/11591/2019, regarding E.E.E., DNI ***NIF.2, line ***TELE-

PHONE.3, it is requested:

- Channel through which a change of address was requested and processed on 07/10/2019.

SIM.

- If the channel was (...) provide the same documentation as that required

in POINT 1. A of this document, if it was (...), documentation required

read at POINT 2. B.

POINT 3

A. Information on whether it is possible to acquire SIM without associating them to any line or

client. Information on whether a customer is allowed to get an unactivated SIM

and without being associated with a specific line, which can subsequently activate telephones.

cally and associate to a line.

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

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

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

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

is not associated with a line or customer during collection (if possible).

ble).

POINT 4

Information on whether fraudulent SIM duplication cases have been detected

in which previously there is a change of ownership supplanting the

identity of the old holder, so that the new holder can subsequently carry out the change

SIM bio.

You are asked to contribute:

A. Security policy that is passed to the applicant in changes of ownership

via (...).

B. Copy of the specific instructions that the operators have in this regard.

beef.

C. Procedure for change of ownership and requirements for applicants

for it.

FIFTH: On January 29, 2020, XFERA requests an extension of the term for

adduce allegations and provide documents or other evidence.

On January 31, 2020, the inspector agreed to extend the deadline

urged.

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

information that was analyzed by this Agency:

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

Required sections according to numbering order:

1.- Information on the routes available to customers:

“(…)”

2.- Detailed information on the procedure:

Duplicate SIM request procedure for YOIGO brand

PRESENTIAL CHANNEL

(…)

NON-PRESENTIAL CHANNEL

(…)

Duplicate SIM request procedure for the MÁSMÓVIL brand

PRESENTIAL CHANNEL

(…)

NON-PRESENTIAL CHANNEL

(…)

Duplicate SIM request procedure for the LLAMAYA brand

PRESENTIAL CHANNEL

(…)

NON-PRESENTIAL CHANNEL

(…)

Procedure for requesting a duplicate SIM card for the LEBARA brand

PRESENTIAL CHANNEL

(…)

NON-PRESENTIAL CHANNEL

(…)

3.- Information on the instructions issued to the operators: it consists of passing the

security policy for both SIM request and activation. It is verified that said

policy is:

(…)

XFERA representatives state that through the tool ***HE-

RRAMIENTA.1 has been sent to all internal and external agents the new

protocols to follow in the event that a duplicate SIM card is requested.

They provide the following documents:

~ Screenshot of the communication sent to all internal agents and

about the existence of these policies, indicating that this communication

tion was sent to all external providers in order for them to

pass on to their employees.

~ Cases in which it must be requested by the telephone operators or through

through the face-to-face channels the approval of the security policy of all

the companies of the MÁSMÓVIL Group for the duplication of SIM Cards.

~ MÁSMÓVIL procedure to request a duplicate SIM Card.

~ YOIGO procedure to request a duplicate SIM Card.

All these procedures have in common the need for the user to provide

the same information that was given to XFERA at the time of contracting or

sale of prepaid SIM card.

In no case is information provided to the client, limiting the operators of

XFERA to carry out this verification.

They provide a copy of two reminders sent on the policy and procedures to

continue.

4.- Information on carrying out the controls:

Controls and requirements established on the shipping address for the remittance of

SIM cards by mail.

Apart from the specialties that have already been detailed for each brand, with ca-

In general, the following aspects are fulfilled:

(…)

They provide a copy of examples of the Delivery Notes.

(…)

During 2019, the protocol to be followed has been reinforced at different times

in the case of Duplicate SIM in the face-to-face channel for the different brands.

The actions, aimed at ensuring the rights of customers, most relevant

During 2019, the following were carried out by each of the brands:

(…)

They provide recording “(…)” as an example of recording a request for a duplicate of

SIM of MÁSMÓVIL to certify the controls that have been implemented.

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

number of clients:

The cases in which this type of action has taken place despite the controls

established are the following:

(…)

6.- Actions undertaken by the entity:

They provide an impression of a procedure distributed among the Customer Service teams

client. It specifies the follow-up that is carried out when the department

of fraud detects a possible impersonation of identity. (...).

In September 2019, new rules began to be designed in the tool

Fraudulent traffic monitoring to detect possible duplicates

fraudulent, (...).

During the month of November 2019, the tool was configured and was being

validating the operation in addition to carrying out active surveillance during

office.

They indicate that on November 28, 2019, the service was opened 24x7 on the platform.

ma Service Control. They provide the current procedure manual. In it you learn

cyan various performances, (...). The last (...) are also analyzed, and if there is no

The client is contacted to confirm.

They state that in order to demonstrate the establishment of controls,

provide three recordings of telephone conversations with the client during the

monitoring process for verification:

~

~

~

Verification call after alarm: with the result of false positive.

Verification call after alarm: with the positive result and fraud

confirmed.

Call received to restore service after preventive lockout

vo, motivated by alert analysis without having been able to verify with the client

tea.

Some identifying features of a position are also exposed in the procedure.

possible fraudulent SIM change, such as the change to electronic format of the

bill, email account change, pre-SIM change events

with incoming calls to the line from suspicious places, and calls after the

change of SIM to customer service of financial institutions.

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

ted throughout the year 2019, the entity has stated: Total cases (...).

(…)

Regarding the total number of mobile telephony clients of the entity, they have stated:

POSTPAID: 4,739,191 Customers.

PREPAID: 1,758,708 Clients

Regarding the cases presented to the agency:

CLAIMANT PARTY ONE:

They provide a copy of the DNI theft report to the police as well as a copy of the DNI (the

SIM duplicate applicant would provide a photocopy of the DNI and not the original since

stating that it had been stolen from him). XFERA representatives indicate that

your fraud department sees indications that the complaint and its accompanying document

to (DNI) are falsified.

CLAIMING PARTY TWO:

XFERA representatives indicate that the request was made by telephone, not

face-to-face as the claimant has stated. They provide recording of the call.

Listening to the recording, it is verified that the operator asks (...).

On other cases not filed with the agency:

Provided the required list, it is verified that there are 20 cases (...).

XFERA representatives indicate that of the 20 cases, only 2 have been claimed.

two, stating that the group has a fraud detection tool and

Most cases of SIM swapping are detected this way, not by claims.

tion.

The following is verified:

(…)

XFERA has also been required to provide a copy of the fifteen cases of (...)

of the recording of the call where the applicant passes the security policy, (...).

It is verified, by listening to the ten calls provided, that all are re-

refer to the activation of the card, already in the possession of the applicant, who usually mentions that

He received it by courier. The following is verified case by case:

CASE 1. (…). The applicant also asks for no. bank account,

mention that it starts with four certain digits and the operator answers

affirmatively.

CASE 2. The operator asks for the name and the applicant says it without surnames.

(...). The operator mentions that the card is usually sent activated.

CASE 3. The operator asks (...).

CASE 4. The operator asks (...).

CASE 5. The operator asks (...).

CASE 6. The applicant says DNI, name and surnames and line number.

CASE 7. Question no. Line. At no time does he ask (...). The operator

calls the applicant by his first name. The operator tells you the new PIN of

the card without asking the applicant.

CASE 8. Question (...).

CASE 9. Question (...). The applicant asks for the invoice amount of 51.33

euros and postal address to which it was sent. The operator tells you the address

invoice delivery.

CASE 10. Question (...).

Of the remaining five cases, no recordings are provided.

Of the ten cases provided, on three occasions the operator did not pass the security policy.

complete security (...). All the cases are from the MÁSMÓVIL and YOIGO brands. In

In two cases, the agents provide data.

It is observed that operators sometimes provide data to the caller despite

include in the security policy that personal data should not be provided in any

In some cases, even beyond the policy.

It is observed that the operators sometimes (...), referring the requestor of the activation

that he was with another operator activating the SIM and the call was cut off, or that they

sent the SIM by courier and was told that he had to call to give the ICC, or

other circumstances. In no case does the operator say that the SIM is worthless or incorrect.

correct because it does not have the ICC number or is not registered for that client or line, simply

Simply associate the new ICC number to the customer's line in the system.

XFERA has been asked about the possibility of acquiring SIM without associating any policy.

line or customer, and information on whether a customer is allowed to get a SIM without activation.

var and not associated with a specific line, which can later be activated by telephone-

mind and associate to a line, as well as if there is a possibility, without SIM fraud swa-

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

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

The representatives of XFERA have stated in this regard that:

(…)

SEVENTH: On August 27, 2020, information is obtained from the Commission

National Markets and Competition on mobile voice lines

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

OPERATOR

MASMOVIL Group

PREPAID

Residential

1,761,276

Business

0

POSTPAID

Residential

5,565,794

Business

19,416

EIGHTH: On January 27, 2021, commercial information on the

XFERA's sales volume during the year 2019 being the results of

1,598,873,000 euros. The share capital amounts to 1,000,000 euros.

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

a sanctioning procedure against XFERA, for alleged violation of article 5.1.f)

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

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

of 500,000.00 euros (five hundred thousand euros), without prejudice to what may result from the

instruction.

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

do in article 77.2 of the RGPD communicates to the CLAIMING parties ONE and TWO

the initiation of sanctioning file PS/00027/2021.

ELEVEN: The Start Agreement is notified to XFERA, on February 15,

2021, through the Electronic Notifications Service and Electronic Address Enabling

litada, according to the certificate that appears in the file.

TWELFTH: On February 22, 2021, XFERA requests the extension of the plan

zo to adduce allegations.

THIRTEENTH: On March 1, 2021, the instructor of the procedure

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

with the provisions of article 32.1 of the LPACAP.

The Expansion Agreement is notified to XFERA on March 1, 2021.

FOURTEENTH: On March 8, 2021, this Agency received, in

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

after expressing what is appropriate to his right, he ends up requesting the filing of the actions

situations, without the formulation of the Resolution Proposal being necessary, due to

that the Proven Facts do not constitute, in a manifest way, an administrative infraction

tive; subsidiarily, the filing of the proceedings is proposed, due to the absence

of guilt on the part of XFERA; and subsidiarily, a sanction is proposed

milder than that included in the Start Agreement.

In summary, he argues that:

PREVIOUS.- PRELIMINARY ASPECTS.

a) NECESSARY SUSPENSION OF THE PRELIMINARY PROCEDURE-

CRIMINAL DAD.

Within the framework of the investigation, XFERA was required to present

a “list of 20 cases of SIM duplicates denounced/claimed as

identity theft or fraudulent by customers”. This listing was

taken into account by the Agency, both for evidentiary purposes (for the purposes of "verifying

compliance with the procedures by the managers of the applications

des”, page 35 of the Agreement) so as to determine the seriousness of the infraction

and its consequent pecuniary sanction (it is considered that the facts occur

“until April 12, 2020 [last of the cases filed with the

agency]”, page 45 of the Agreement). Among the cases that make up this list are

finds the one related to the line number ***TELEFONO.5, which occurred on the 14th of
January 2020 and related to the DNI ***NIF.3. This case is being investigated
criminally, and specifically, by the Investigating Court No. 9 of Ali-
cante, within the framework of the preliminary proceedings ÑÑÑÑÑ/ÑÑÑÑÑ. is accompanied,
as Document 1, official letter of the aforementioned court addressed to our company that
confirm this fact.
The modus operandi of this assumption is identical to that identified in the case of the
CLAIMANT PARTY ONE: person who goes to a Yoigo store to request
cite a duplicate of a SIM card, providing a supposedly falsified DNI
down to identify. It is XFERA's opinion that it is decisive in resolving
see the file to prove whether the events actually occurred in the way
described, because if this end is confirmed, the absence of guilt of
XFERA would be evident, which would necessarily entail archiving the experience.
tooth. It is alleged that while a criminal proceeding is pending for the
investigation of such facts, any administrative action must be suspended.
sanctioning as long as criminal liability is not determined elucidated-
gives. All of this while awaiting a firm judicial resolution, the facts of which have been declared
proven will bind this Agency with respect to this sanctioning procedure.
in accordance with the provisions of article 77.4 of Law 39/2015, of 1
October, of the Common Administrative Procedure of the Public Administrations
(hereinafter, LPACAP). Therefore, the suspension of the period of
resolution of the file until a sentence falls on the indicated process.
criminal proceeding.
b) DISCONFORMITY WITH THE ACCUMULATION OF FACTS IN THE PRE-
SIT FILE.
XFERA expresses its disagreement with the accumulation of the facts of the

that brings cause this file in a single administrative procedure, all

once it considers that the requirements set forth in article 57 are not met

of the LPACAP. Said article reads as follows: “The administrative body that

initiate or process a procedure, whatever the form of its initiation.

ciation, may dispose, ex officio or at the request of a party, its accumulation to other

with whom it maintains a substantial identity or intimate connection, provided that it is the

same body that must process and resolve the procedure. Against the agreement

of accumulation, no recourse will proceed”. XFERA considers that the

facts analyzed here do not keep "substantial identity", because they bring cause

of two very different situations that can be summarized in that, in one of

cases, XFERA was the victim of alleged crimes of falsifying documents

official and identity theft, whenever the employees of one of its

stores were deceived by a person who exhibited a complaint and a Do-

manipulated National Identity document, which has a decisive impact on

the unlawfulness and culpability of XFERA in relation to the infraction that

is attributed to him, while, in the other case, the deception occurred over the phone,

because the applicant had an unactivated SIM card and recited

correctly all the digits of your ICCID, so there was no deviation

of the established procedure regarding the change of telephone SIM in that

moment. Article 85 of the LPAC grants the offender the right to acknowledge

certify their responsibility and to proceed to the voluntary payment of the pecuniary sanction

proposal, with the legally foreseen reductions. In this regard, XFERA does not

cannot and should not acknowledge its responsibility in the first of the ex-

positions, because it is evident that he lacks any culpability in relation to the

infringement attributed to it. However, by accumulating the actions, it has become

violated their right to acknowledge responsibility and proceed to pay voluntarily.

laughed about the second of the exposed facts. Every time against the accumulation

tion of infringing acts in a single procedure there is no appeal,

records this disagreement from the initial moment of the procedure.

administrative proceedings, as well as defenselessness and violation of rights

that causes XFERA, in order to be able to use this argument in the possible

challenging the resolution issued by this worthy Agency to put an end to its

processing.

FIRST.- WHAT IS SIM SWAPING?

The English expression "SIM swapping" is used in our country to designate a type

of

cyber-fraud, which is described by the National Police as follows: “The method used

for the scam consists of several phases; In a first phase, those investigated seized

raban of the access codes to the online banking portals of the different entities

by means of “phishing”, “malware” or “pharming” techniques. got the keys,

the authors requested a duplicate of the SIM cards of the different victims,

providing mobile phone companies with false documentation -in some cases,

even from public figures - with the intention of receiving the confirmation codes of

the fraudulent transfers that they later made. Obtained those codes

gos, made the fraudulent transfers from the accounts of the victims to

third-party accounts, which they used to channel the money. On other occasions

sions, they also requested pre-approved loans or microcredits from entities

banks, in order to obtain greater economic benefit. All this was done in

a short period of time, between one and two hours; maximum time in which the victim

he realized that his phone had stopped working -because his SIM card is-

was inactive-because it was already operating with the new duplicate card”

(https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=8081).

As can be seen, the commission of this crime entails carrying out a whole series of

criminal conduct, which begins with the criminal's access to information

personal information and bank passwords of the victims, go through the usurpation of the identity

victim's authority to get a copy of their SIM card, and end up with receiving

on a mobile device of the confirmation codes necessary to authorize the

making transfers. It is a form of fraud that, as stated

increase in

the report of the year 2020 of the Prosecutor's Office, referring to the year 2019, "is generating justification

cares about your

last annual period” (

https://www.fiscal.es/memorias/memoria2020/FISCALIA_SITE/recursos/pdf/

capitulo_III/cap_III_8_2.pdf, p. 1011).

XFERA considers it important to clarify that obtaining by the perpetrators of the du-

The application of the SIM card is a means for the commission of the crime, which occurs only

directly after having obtained the passwords and personal information of the victim. And that the

practice was extended in 2019, as a result of the precipitated implementation by the

financial entities from the so-called “reinforced authentication obligations” foreseen
ts in Directive (EU) 2015/2366 (known as PSD2), which entered into force on 14
September of that year. This was so given that the method chosen by the banks,
against the criteria of public cybersecurity organizations such as Incibe, was the call
mada "authentication in two steps" by sending keys by SMS; A technique
clearly vulnerable, as has been shown in practice.

a) SIM CARDS ARE DUPLICATED THROUGH COUNTERFEITS.

It must be assumed that the cybercriminal already had in his possession the
personal data of the affected party necessary to duplicate the SIM card and thus
recognizes the Agreement itself (page 31): “It should be noted that for the sub-
planters can carry out fraudulent banking operations, in addition to
duplicate the SIM card of the affected people, they must have in their possession
other data, specifically the banks with which these people operate and the
online banking access credentials, since access to messages
SMS by itself does not allow the execution of banking operations”. of this
So, in order for a scammer to get a duplicate SIM, they must generate
generate sufficient elements of presumption of identity of the affected party, providing
data such as a copy of your ID, your own telephone number or identification data
relating to the victim that exceed the control measures implemented for this
process. Such is the case that, if these data are not previously available, the so-called
"security procedure" would block any access attempt. In defi-
tive, the confidentiality of the data has not been compromised for any reason
attributable to XFERA, since it was previously committed.

b) TWO-STEP SMS AUTHENTICATION IS INHERENTLY
INSECURE.

Since 2017, the National Institute of Standards and Technology of the Es-

United States (NIST) believes that the use of public telephone networks

switched for sending authentication codes (for example, through

SMS)

(watch

regard:

https://pages.nist.gov/800-63-3/sp800-63b.html#restricted).

Around the same dates, the National Cybersecurity Institute of Spain (Inci-

be) published on his blog, when talking about two-factor authentication: “The me-

two-step canisms are more vulnerable and discouraged, being able-

communication of the second factor is intercepted because it is usually something that we

send,

SMS"

(https://www.incibe.es/protege-tu-empresa/blog/dos-mejor-uno-doble-factor-

access-critical-services).

However, and despite these warnings, the financial institutions are considering

Considering that the sending of an authentication code by SMS complies with the

www.aepd.es

sedeagpd.gob.es

usually

restricted

must

to the

by

be

criteria established in the PSD2 Directive to be considered a mechanism
of "strong authentication". Thus, they began years ago by offering their
customers the possibility of using this method of identification, for more recently
he is afraid to impose it on his entire clientele.
The entry into force of these strong authentication obligations is not pro-
lasted until September 14, 2019; but many financial institutions
advanced to that date. It is in this context that crime is popularized.
known as “SIM swapping”.
With the adaptation to PSD2, the criminals also needed to access the
SMS that banks sent to users, then beginning to supplant
identity of said victims to try to obtain from the operators during
applications of your SIM cards. Companies like XFERA suddenly found themselves
with a new criminal operation that, until now, has simply been unknown.
they knew; and it is precisely in this temporal context that the
the facts denounced by the claimants, since the complaint of the
CLAIMANT TWO refers to events that occurred on September 25
of 2019, and the one presented by the CLAIMANT party TWO deals with facts
occurred on July 10, 2019.
SECOND.- XFERA ADEQUATELY MANAGED THE RISK IN RELATION TO
WITH SIM-SWAPPING.
XFERA alleges that the facts brought about by this proceeding should be divided
in two clearly differentiated periods: the one prior to the knowledge by
XFERA of the criminal operation known as “SIM swapping”, and the one after the
identification of said risk. The reality is that XFERA has no effective knowledge
of this problem until September 26, 2019, when it receives a request

ment of the General Subdirectorate of Attention to the Telecommunications User, of
the Secretary of State for Digital Advancement (SEAD), which begins as follows (it is
accompanies a copy of the aforementioned request as Document 2): "In this Subdirectorate
General queries and complaints have been received about a fraud with the following-
operative te: certain personal data of a user is previously obtained
(such as the DNI, or current account number). Based on these data, who has the
intention to commit fraud requests the operator, with the personal data previously
mind obtained, a duplicate of the SIM card. From there, once achieved,
financial transactions can be made by accessing financial services by
Internet, since these include as a security mechanism, the achievement of
a key that is sent to the mobile phone (which would be accessed by duplicating
of the SIM card)". Given this news, XFEA activated a review procedure
of its security measures, in line with the risk management obligations and
active responsibility established by the RGPD. On the one hand, the pro-
identification procedures, collected on pages 16 and following of the Agreement; Y
on the other, two additional layers of security were activated, which began to be applied
on November 28, 2019, but even though they are mentioned on page 24
of the Agreement itself, everything indicates that its effectiveness and the effort made by the company
sa for its development have not been sufficiently taken into account by this Agency.
To certify that the review of the security measures actually took place,
after having knowledge of this problem, the document of analysis of
risks in relation to the treatment of identification of users of XFERA, in its
versions before and after the detection of this criminal operation, such as Documents

ments 3 and 4, respectively.

2.1. SECURITY LAYERS IMPLEMENTED BY XFERA.

The layered security system implemented by XFERA since November 2019 follows the so-called “Swiss cheese model” of risk management. In In this model, an organization's barriers against threats are modeled layered lan, represented as slices of cheese. Be part of the base that no security measure is perfect, so the inherent weaknesses Before each layer they are represented as holes in the cheese slices. Yes the measures implemented in each of the layers are different, the holes numbers will vary from layer to layer. For the security gap to occur ity, the holes in all the slices should line up, so that a attack could pass through them entirely; but the probability that this happens, if the system is well planned, it is extraordinarily low.

The first of the security layers implemented by XFERA, and the only one existing until November 2019 in relation to duplicate cards SIM, is the so-called "security policy", which serves to validate the identity of the appliers. The Agency sees in it "possible vulnerabilities" (page 35 of the Agreement), derived both from human error and from the skill of the criminals to supplant the identity of the victims. However, do not lues the two additional security layers implemented by XFERA, which gives rise to an incomplete analysis of the facts, to the point of qualifying it unfairly as “negligent”.

The second of the implemented layers is based on the so-called principle of “data protection by design”, and consists of a computerized tool

ca named “***TOOL.2”. (...). In the event that a request is

detected as potentially fraudulent, the system launches an alarm,

effects that a technician can check if the case is indeed fraudulent

and apply the relevant protocol. The system is activated based on factors

as the following:

(…)

This system is applied even after the first layer of security has been breached.

by criminal applicants (that is, once the policies have been overcome).

identification cards established in stores and in the customer service

client), and has a very high efficiency. Alerts are monitored by a

technical team, in 24x7 mode and with an established SLA of 5 minutes.

The third layer of security is the random review of those requests for

duplicate card not detected as suspicious by the system “***HE-

TEAM.2”. This review is carried out at night, by the department

service control element, and takes into account factors such as the following:

(…)

The main action, in case of suspicion, is the immediate blocking of the shipment and

reception of SMS messages; In addition to trying to contact the owner of the

line to verify that you have indeed requested a duplicate of your card

SIM (the policy in application is attached as Document 5). Refering to

effectiveness of the measures, the numbers speak for themselves, and demonstrate their role

great success. These are the statistics for 2020:

22/102

Concept

SIM card duplicates made

Quantity

***QTY-

DAD.1

Percentage

***PERCENT-

TAGE.1

DAD.3

DAD.2

TAGE.3

TAGE.2

***QTY-

***QTY-

***QTY-

***PERCENT-

***PERCENT-

Potentially fraudulent activation attempts

detected

Fraudulent attempts that exceeded the security policy

security (1st layer)

Fraudulent attempts that passed the ***TOOL-

LIE.2 (2nd layer)

Fraudulent attempts that passed random review

toria (3rd layer)

The conclusions that can be drawn from these statistics are the following:

 While the total number of fraudulent card duplication attempts

SIM rates is high, it represents a very small percentage of the immense

volume of legitimate requests that XFERA receives annually.

The security policy applied by the company, in general,

It is very effective: (...). The effectiveness of this measure was therefore

***PERCENTAGE.6.

***PERCENT-

***PERCENT-

***QTY-

TAJE.4

TAGE.5

DAD.4

DAD.5

 The ***TOOL.2 system has also demonstrated its effectiveness:

(...) for this second filter. Its concrete effectiveness was, therefore,

***PERCENTAGE.7.

 Regarding the random reviews carried out by the department

service control element, (...), with an efficiency of ***PERCENT-

JE.8.

As can be seen, and in summary, the implementation of the cheese strategy

Swiss worked with a cumulative efficiency of ***PERCENTAGE.9; and guessed

an effective reduction of ***PERCENTAGE.10 in cases in which the de-

offenders achieved their illicit goals. Evidently, the objective of XFERA

is to detect 100% of fraud attempts, and we continue to work on that line.

ing ... but it cannot be denied that the results obtained are true-

mind spectacular, and that XFERA has put all its efforts into making

this figure even lower, with each of the measures that have been implemented

tanting Document 6 provides a table with the ***NUMBER.3 cases

who have overcome the first barrier.

2.2) LIST OF THESE MEASURES AND THE TWO CASES IN WHICH

BRING CAUSE THE FILE.

The “Swiss cheese” security model was implemented on November 28,

2019, after XFERA became aware of the existence of the illegal practice

appointment known as SIM swapping. Unfortunately, the reported facts

by the complainants occurred before the application of these measures, and before

even of the reception by XFERA of the request of the SEAD; and if they could

materialize is because XFERA was unaware of this criminal operation and, therefore,

had not been able to take it into consideration when assessing its risks and

establish appropriate security measures. Specifically, faiths

The calls in which the SIM card duplicates were processed were the following:

you:

 In the case of CLAIMANT ONE, on September 25,

2019;

 In the case of CLAIMANT TWO, on July 10, 2019.

However, it should be noted that the circumstances surrounding each

of these cases are very different:

 In the case of CLAIMANT ONE, the criminals managed to

deceive the staff of a Yoigo brand store by training

ga of false documentation, and specifically, of a DNI and a complaint of

theft manipulated by computer programs for the treatment of

images. In this sense, the manipulation carried out fell on ele-

essential elements of the documents provided to store personnel

da, such as the name and surname of the holder of the DNI and the complainant;

and had enough entity to deceive these workers. Re-

In this regard, it is irrelevant that the XFERA fraud department

subsequently appreciate “indications that both had been falsified

ceded” (page 40 of the Agreement), because it is not required of employees

of a store the knowledge about documentary falsities that con-

turns into an expert in fraud detection: on the contrary, the criterion

to employ is the suitability of deception to mislead a person

medium capacity. It is emphasized that the manipulation of said documents

these are not crude unprofessional manipulations, but manipulations

tions made with a degree of detail more than enough so that

a diligent and careful person can take such documents

as true.

To the extent that they are suitable documents to produce a

deception, and that in practice they achieved their goal, XFERA has been a victim

ma of a crime of falsehood in an official document, provided for in article

392 of the Penal Code. Note that the protected legal interest, in the case

of this crime, is the legitimate trust of citizens and institutions

based on the adequacy of public documents to reality:

to consider XFERA responsible would mean ignoring the principle of fault-

bility, and would generate an obvious defenselessness. Hence there is no room to derive

var administrative responsibility for this assumption.

 The case of CLAIMANT TWO, on the other hand, is somewhat more doubtful.

SW.

Everything indicates that the impersonator was made with a "blank" SIM card,

probably after illicitly obtaining it (…). Thus it follows from

content of the call: just listen to the conversation to check

bar that the applicant had the complete ICCID of the SIM card,

which is only printed on the back of the card itself. convie-

It should be noted that the case occurred on July 10, 2019, and was the first

number of this nature that affected XFERA: never before had it been

detected a duplicate SIM in which the applicant had booked

previously and illegally deducted from a non-activated card of this brand. Co-

how the offender obtained it is a complete mystery to XFERA, but

It was probably stolen from a store, or an official installer. Nope-

tese that, at that time, the company did not follow up on

their non-activated cards, because their economic cost is low; because

they are “blank” media, which do not contain any type of information

staff; and because until then no similar frauds had been detected.

similar to that described in this procedure. It had not been perceived, in short,

tive, a risk related to this type of element. In practice,

back then, there was only one legal method to get a SIM not

activated: having received it through the “***SERVICIO.1” service, after

have requested it by phone. The form of delivery, in itself, constitutes

constitutes a security measure, since it requires the display of the document

of identity in force, coinciding with the number of the document of

identity of the owner of the line; and for that reason, until then the

agents received only genuine calls: hence the laxity of the traffic.

telephone activation limit. It was as a result of the beginning of receiving

requests of this type when the security procedure was modified.

ity, expanding the need to adequately identify the applicant

all kinds of cases. However, anticipating this criminal operation in the

At the time this incident occurred, it was simply impossible.

ble for XFERA. This Agency cannot pretend to impose obligations

results, excluding from the equation the necessary component

subjective and the clear diligence shown by XFERA, when only

has suffered a handful of cases while boasting a client base.

you have more than 7 million mobile lines. That said, with the system

theme implemented at the end of 2019, with total security the second

of these two cases would not have occurred, and very likely, also

little the first. Hence, it is understood that the problem of security

dad has already been corrected.

2.3) RELATIONSHIP BETWEEN THESE MEASURES AND THE 20 ADDITIONAL CASES,

CONTRIBUTED TO THE AEPD.

In its request of June 18, 2020, the AEPD asked XFERA to

provide a “list of 20 cases of SIM duplicates reported/claims

two as identity theft or fraudulent by customers". compliant

With the request, we send the Agency the list of requested, accompanied

accompanied by an explanation of great relevance, which is ignored in the process.

ment. We transcribe it again, so that it can be taken into account

by the Instructor: "Beforehand we consider it necessary to clarify the

Next information. We provide a list with the first 20 application cases

SIM duplicate confirmed fraudulently. XFERA has a

fraud detection tool that has the ability to detect, among

other things, (...), in order to avoid fraud. This alert is transferred to

customer service to get in touch with the customer and

make the necessary checks, opening a Claim ticket in

***APPLICATION.1. The vast majority of claims for SIM Swapping

are initiated in this way and not through a claim or complaint made

given by the client, in fact, as can be seen in this list, only two of

the cases we report have been claimed or denounced directly

for the client". As can be seen, the writing is clear in informing the

Agency that they were being provided with the first twenty cases detected

by XFERA, but only two of them corresponded to cases de-

reported or claimed by customers, because the remaining eighteen were

detected almost immediately by the fraud detection tool

***TOOL.2, which, as we have explained previously, was developed

given by our company, and implemented on November 28, 2019.

A table is reproduced below where the twenty

claims submitted at the time to this worthy Agency, but incorporated

telling them the date and time the illicit request was received and the

SIM card lock. It is noteworthy that three of the numbers

ros are repeated, because the fraudulent operation was intercepted in two

occasions by the security system:

MSISDN

***PHONE.4

BRAND

MoreMobile

CHANNEL

Telephone

***PHONE.5

Yoigo

Store

***PHONE.6

MoreMobile

Telephone

***PHONE.7

MoreMobile

Telephone

***PHONE.8

Yoigo

Telephone

***PHONE.9

MoreMobile

Telephone

***PHONE.10

***PHONE.10

***PHONE.11

***PHONE.12

***PHONE.13

***PHONE.14

***PHONE.15

***PHONE.15

***PHONE.16

***PHONE.12

***PHONE.17

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Store

Store

Store

Telephone

Telephone

Telephone

Telephone

Telephone

Telephone

Telephone

Store

Request

05/01/2020

22:12

01/14/2020

20:18

01/15/2020

12:43

01/20/2020

21:01

01/25/2020

16:48

01/27/2020

14:20

01/27/2020

17:07

01/27/2020

19:56

01/28/2020

12:29

02/04/2020

16:08

02/25/2020

23:05

02/27/2020

18:31

02/29/2020

21:38

03/03/2020 7:37

05/03/2020

17:07

05/03/2020

21:07

03/11/2020

Blocking

05/01/2020

22:24

01/15/2020

21:43

01/15/2020

13:20

01/20/2020

22:51

01/25/2020

17:50

01/27/2020

17:50

01/27/2020

17:28

01/27/2020

21:50

01/28/2020

12:59

02/04/2020

16:26

02/25/2020

23:12

02/27/2020

19:19

02/29/2020

21:51

03/03/2020 7:48

05/03/2020

22:23

05/03/2020

21:37

03/11/2020

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

***PHONE.18

Yoigo

Telephone

***PHONE.19

MoreMobile

Telephone

***PHONE.20

MoreMobile

Telephone

***PHONE.21

***PHONE.22

Yoigo

Yoigo

Store

Telephone

13:59

03/13/2020

12:51

04/03/2020

15:11

04/04/2020

13:45

04/08/2020

21:03

04/12/2020

15:39

14:42

03/13/2020

13:24

04/03/2020

15:22

04/04/2020

14:04

04/08/2020

22:04

04/12/2020

15:54

As can be seen, the effectiveness of the second layer of security is very

high (greater than 90%, according to our calculations), and is summarized below.

tion:

 In the following cases (a total of 10 out of the 22 listed above-

mind), the ***TOOL.2 system detected the possible fraud and the

XFERA personnel managed to contact the owner of the line, blocking

the duplicate card before the criminals achieved their goal,

as far as we know: ***PHONE.4, ***PHONE.8, ***PHONE-

PHONE.10 (on two occasions), ***PHONE.11, ***PHONE.14,

***PHONE.18, ***PHONE.19, ***PHONE.21, ***PHONE-

PHONE.22. The mean block time, in the listed cases, was 40

minutes; and its median, 31 minutes.

 In the following cases (a total of 9 out of the 22 listed above-

te), the ***TOOL.2 system detected the possible fraud and, despite

that XFERA personnel were unable to contact the holder of the

line, the ability to receive SMS on the duplicate card was blocked

before the criminals achieved their goal, as far as we know-

mos: ***PHONE.6, ***PHONE.10, ***PHONE.12 (in two

times), ***PHONE.13, ***PHONE.15 (on two occasions),

***PHONE.17, ***PHONE.20. The average block time,

in the cases listed, it was 43 minutes; and its median, 19 minutes.

 In the case of the number ***TELEFONO.16 (1 over 22), the

***TOOL.2 did not detect the possible fraud, but the autho-

XFERA service control audit (third security layer),

blocking the duplicate card. It turned out to be a “false positive”: the customer

contacted the company days later, to request its unlocking.

 In the following cases (a total of 2 out of 22), the ***TOOL-

LIE.2 did not detect the fraud, and it was the clients themselves who

contacted XFERA, after detecting that their line was not working

correctly: ***PHONE.5, ***PHONE.7.

Of these two cases, it is important to note that, as regards the number

telephone number ***TELEFONO.5, identity theft occurred in

a Yoigo store, and that the applicant exhibited a false DNI, whose co-

pia was added to the file. They are considered reproduced, in this regard,

the allegations raised in relation to the case of the CLAIMS party

KEEP ONE, in relation to the absence of illegality and culpability

in the conduct of XFERA.

This significant improvement in procedures has not been analyzed by the

Spanish Agency for Data Protection in its Start Agreement, despite

than the existence of the fraud detection system (...).

It is important to note that the last case, among those requested by the Agency

ence, in which the applicant managed to overcome the two layers of security, the

January 20, 2020. In this regard:

 It is evident that the “improvement” claimed in the Agreement (page 37)

has already happened, and security continues to increase every day that

happens, as errors are used to proactively calibrate

the ***TOOL.2 system, and make it more and more efficient; Y

 The period of duration of the alleged infraction collected is incorrect

on page 45 of the Agreement, since the last of the cases provided

two in which fraud was confirmed occurred on January 20, 2020, and

not on April 12, as the resolution indicates.

2.4) INCORRECTNESS OF THE SPANISH AGENCY FOR THE PROTECTION OF

DATA.

The inconsistency of the sanction proposed in this file is striking,

in relation to other resolutions on analogous cases, in which the effort

security measure carried out by XFERA was taken into consideration by the

Agency and took to the file of the proceedings. Take as an example the recent

resolution dated February 15, 2021, in file E/09594/2020, re-

relative to a supposed "absence of security measures with the consequence

of issuing a duplicate SIM card without the consent of the claimant”, which

concluded with the inadmissibility of the claim based on the following grounds:

tation: “The processing of the claim in accordance with the provisions of article

65.4 of the LOPDGDD, has led to the solution of the issues raised

das, without the need to purge administrative responsibilities in the framework

of a sanctioning procedure. In this regard, it is worth mentioning the

exceptional nature of the sanctioning procedure, from which it derives that -always

whenever possible-the prevalence of alternative mechanisms should be chosen.

in the event that they are protected by current regulations, as occurred

rre in this case. In short, the applicable principles should be brought up

to the penalty procedure. The Spanish Data Protection Agency

exercises the sanctioning power ex officio. Therefore, it is exclusive jurisdiction

of the Spanish Agency for Data Protection assess whether there are responsibilities

administrative data that must be purged in a sanctioning procedure

dor and, consequently, the decision on its opening, there being no obligation

to initiate a procedure before any request made by a third party. such-

The decision must be based on the existence of elements that justify said initiation

of the sanctioning activity, circumstances that do not concur in the present

case, in view of the actions carried out, so the filing of

the claim filed against XFERA MÓVILES, S.A.”

It does not seem reasonable for the Agency to understand, on the one hand, that the questions

issues raised in relation to security measures are resolved and that

It is not appropriate to open a file, given the exceptional nature of the procedure

sanctioning; and on the other, that identical measures are insufficient and should be sanctioned.

join XFERA. Especially when both resolutions were notified on

the same day.

2.5) THE FIVE MISSED CALLS HAVE BEEN LOCATED, AND

CONTRIBUTE NOW TO THE FILE.

The Agreement states, on page 40, that “in five of the cases [additional

provided by Masmóvil] not even the calls protected by the

in possible errors in their coding (nomenclature). The

so-called “encoding errors” occur when the call is made

from a line other than the one the query is about, and the operator

rador does not record this circumstance manually in the systems of

company customer service. However, the calls in question

are stored on the servers, and although locating them entails an arc

duo search process, it has been possible to recover them: they are now contributed to the ex-

pending, as additional evidence, as Documents 7, 8, 9, 10 and 11.

Its content is summarized:

CASE 1: It corresponds to the line (MSISDN) ***TELEFONO.4, and there was

on January 5, 2020. The operator asks for (…). The applicant responds

correctly to the first two questions, but mentions that he only remembered

memory of the last three digits of the line number.

CASE 2: It corresponds to the line ***TELEFONO.7, and it occurred on the 20th of

January 2020. The operator asks for (…). The applicant answers correctly-

mind to the three questions.

CASE 3: It corresponds to the line ***TELEFONO.10, and it occurred on the 27th of

January 2020. The operator asks for (...). The applicant answers correctly

to all three questions. The operator doubts, because the sending of the duplicate

of the card does not appear in the system and requests instructions from its coordinator.

This confirms that if the applicant exceeds the security policy, it can be

activate the card.

CASE 4: It corresponds to the line ***TELEFONO.13, and it occurred on the 25th of

February 2020. The applicant provides the DNI and the last three digits of the number

river of line The operator doubts, because the sending of the duplicate of the card does not

is in the system. After being asked, the applicant also provides the name

full name of the owner.

CASE 5: It corresponds to the line ***TELEFONO.19, and it occurred on the 3rd of

April 2020. The operator asks for (…). The applicant answers correctly-

mind to the three questions.

As can be seen, the applicants knew, in all cases, the data

ID number and name and surname of the holders of the line, thus overcoming the

initial security policy (first layer) of the company. Now of these

five assumptions, four were intercepted by additional layers of se-

security, and mainly, by the ***TOOL.2, which undoubtedly gives a

a very rough idea of the focus XFERA puts on implementing effective measures

you go and the success of the same to reduce to the minimum expression any type

spoofing in the SIM duplication process.

THIRD.- THE ACTIVATION OF A DUPLICATE SIM CARD IS NOT

A TREATMENT".

It is stated in the Agreement (page 32), that "it is crystal clear that the data

that are processed to issue a duplicate SIM card are personal data,

and its treatment must be subject to data protection regulations. Without em-

However, that "meridian clarity" that the Agency affirms should be applied, only,

to the identity verification process prior to the activation of the duplicate card

SIM: the activation itself cannot and should not be considered a “treatment”, and in fact

cho, the Agreement does not justify at any time that it is so.

A SIM card is a mere medium, an encrypted device designed to store

inside it a code called IMSI (International Mobile Subscriber Identity) and a

associated cryptographic key. As explained by the National Markets Commission and the

Competition on your blog, the IMSI is a fifteen-digit code, consisting of the following-

following: “The first three digits define the country and are called MCC (Mobile Country

Code) or IPM (Country Code for Mobile service). The MCC/IPM of each country

assigned by the ITU and that of Spain is number 214. It is followed by the number indicated by the operator.

rador, which in Spain is assigned by the CMT. It is the MNC (Mobile Network Code) or IRM (In-

indicative of the Mobile Network), of up to three figures (in Spain it is two). The remaining digits

Many are the MSIN (Mobile Subscription Identification Number) and are reserved for

the operator assigns them to each of their customers' lines."

An XFERA technician internally assigns this generic IMSI to one or more

MSISDN (the user's line number); but (1) IMSI and MSISDN are numbers

different, and (2) the latter is not stored on the SIM card, as collected by the same

CNMC article: “Our phone number is not stored on the SIM card

MSISDN, but instead it is essential that the IMSI is present (in addition to the ICCID and

other data). In case of theft, if we inform the operator that our SIM has been

stolen, he will give us a new SIM with a new IMSI to prevent someone

can make calls on our behalf. However, we will keep our

MSISDN (...) In addition, as we have mentioned before, different IMSI numbers (of different

different subscriptions) can point to the same telephone number."

In all 15 telephone calls examined by the Agency in the framework

of the procedure, there was the circumstance that they were in the possession of the applicant

SIM cards not activated, without XFERA being able to know how to obtain the

themselves (although it is believed that they were stolen, either in a store, or from some

authorized logger); but such cards are blank, and (1) do not contain any

type of personal data; (2) do not have any type of identifier associated

directly or indirectly, to any interested party; and (3) do not allow access to in-

training relating to any natural person.

As for the activation procedure, it simply involves associating the IMSI code

already included in the SIM with an MSISDN; and it is an exclusively technical process.

co, which does not entail any type of operation "on" personal data; something extraordinary

unrelevant, because it excludes the existence of a "treatment". Notice that,

According to article 4 of the RGPD, the definition of treatment is the following: "«treatment-

ment»: any operation or set of operations performed on personal data

data or sets of personal data, whether by automated procedures or not,

such as the collection, registration, organization, structuring, conservation, adaptation or

modification, extraction, consultation, use, communication by transmission, diffusion or

any other form of authorization of access, collation or interconnection, limitation, su-

pressure or destruction;"

The mere fact that the MSISDN can be considered personal data does not entail
that it is a "treatment" and that, therefore, the protection regulations are applied.
data tion: this will only happen when operations are performed on data
personal. The reality is that, when a SIM card is activated, no operation is performed al-
any information about the MSISDN, or about any other personal data: only
acts on the card itself, and this cannot be considered “data of a personal nature”.
nal”, nor does it contain information of this nature. A SIM card is not data, it is a
support, and when it is first activated, it is empty of all content. I do not know that,
therefore, before a treatment; and for that reason the RGPD should not apply to the
specific operation of activating the SIM card.
Obviously, it cannot be denied that, prior to said activation,
conducts personal data processing by XFERA, consisting of verifying
the identity of the client. At that moment, effectively, operations are carried out on
about the personal data of the owner of the line, and there is no problem in admitting the
application of the RGPD to that phase of the procedure object of analysis in the present ex-
pending. But the treatment in question ends with the owner's own identification:
the activation of the SIM card is later in time and, in no case, should it be
considered a "treatment" of personal data. This approach apparently
insignificant, it reverts great importance, because from it derives the risk that XFERA must
consider for the purposes of establishing the applicable security measures.
FOURTH.- APPLICATION TO THE CASE OF THE PRINCIPLE OF PERSONALITY.
Article 28 of Law 40/2015, of October 1, on the Legal Regime of the Sector
Public (hereinafter, LRJSP), which “may only be sanctioned for acts constituted
tutives of administrative infraction the natural and legal persons (...) that result
responsible for the same by way of fraud or negligence”. This article consecrates the so-called

“principle of strict sanctioning responsibility”, or “principle of personality”, pre-

seen in article 25.1 of our Constitution. It is one of the pillars of the

punitive law of the State, which entails “the impossibility of transferring the consequences

sanctions against persons or entities other than the perpetrators of the crimes

punishable acts”, in the words of the National High Court, which cites the doctrine of our

Constitutional Court on the matter as follows: “The ruling of the Constitutional Court

tional 219/1988, of December 22, proclaimed that the principle of personality of

sanctions or personal responsibility for own actions prevents an undue

transfer of punitive responsibility to a person unrelated to the infringing act, since this

would entail accepting a regime of strict liability that would violate the

evidence of fraud or negligence necessary for the existence of an administrative infraction”.

XFERA considers that the Agreement, strictly speaking in defense terms, violates

said principle; and this because it links the seriousness of the alleged infraction, not to the treatment

data processing carried out by XFERA in itself considered, but to the consequences

illicit use of the duplicate SIM card by third parties. It

does, in fact, on multiple occasions, and among them:

 On pages 45 and 46, where when analyzing the aggravating circumstances of the

case, mention the following:

o Nature, seriousness and duration of the infraction: The Agency considers

that the nature of the infraction is very serious since it entails a

loss of disposal and control over personal data”.

As has been exposed, the SIM cards that duplicate cybercriminals

are blank, and therefore lack any personal data in

its interior. Therefore, access to a copy of the SIM card, in itself,

does not imply any type of loss of disposition or control over data

personal. Please note that cyber fraudsters can only obtain

have such a copy if they have previously managed to intercept the personal data

data of the interested party by other means, through techniques such as phis-

hing(acknowledged by the Agency on page 31 of the Agreement). It of-

shows that the loss of disposal and control over personal data

happened to them prior to the events that this excerpt deals with.

pending, and brings cause of the action of a third party unrelated to XFERA. Attri-

assigning this responsibility to XFERA is simply contrary to law.

cho.

o Level of damages suffered: High. Drift in operations

fraudulent bank transactions that happen in a short space of time. I-

Through the duplication of SIM cards, the supposed impersonators

get control of the subscriber's line and specifically the reception

of SMS addressed to the legitimate subscriber to carry out online operations

with banking entities supplanting their personality. These SMS

sent by the banking entities as part of the verification in two parts.

operations such as money transfers or payments by Inter-

net, and access to these SMS is often the reason for fraudulent duplication.

dulent of SIM cards".

The consequences derived from crimes committed by third parties

they can be transferred, in the form of aggravation, to XFERA; and this because

It is not possible to attribute subjective responsibility to XFERA for criminal acts.

interests of others, and because strict liability is proscribed in the

penalty procedure.

o Categories of personal data affected by the breach: Access

unauthorized access to a duplicate SIM card is considered particularly

It is serious since it enables identity theft".

As stated, unauthorized access to a SIM card does not

entails access to any personal data. that cyber scammers

use these cards as a tool for committing crimes

It is caused solely by the weaknesses of the security systems

of entities that use SMS as a means of authentication, even

knowing that it is an inherently unsafe method.

Therefore, the responsibility of third parties is once again being transferred

ros, in the form of an aggravating circumstance, to XFERA, violating the constitutional precept

mentioned above.

 On page 33, where the rationale on which the Agency is based for

open a procedure against XFERA:

"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 supplanting person performs the replacement of the SIM, the telephone

of the victim is left without service passing the control of the line to the person

impersonator. Consequently, the claimants are affected by 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
the Constitutional Court in Judgment 292/2000, of November 30,
2000 (FJ7). So, by getting a duplicate SIM card,
impersonators will automatically have access to contacts and will be able to access
to all applications and services that have as a recovery procedure
Password ration Sending an SMS with a code to be able to change the
passwords. In short, they may supplant the identity of those affected,
giving access and control, for example: email accounts;
bank accounts; applications like WhatsApp; social networks, such as Facebook
book or Twitter, and a long etc. In short, once the cla-
sees access by impersonators lose control of their accounts,
applications and services, which poses a great threat."
To the extent that a telephone line is not personal data, the
Affectation for the powers of disposal and control over personal data
of the claimants brings cause of the action of the supplanters, who use the
SIM to change passwords of victims. However, the responsibility
The quality of this conduct is, once again, alien to XFERA, and must be restricted exclusively
tively to the criminals who commit the criminal act, and to the entities
that do not configure secure authentication protocols for the change of
passwords from your customers.
In short, XFERA's actions are limited exclusively to facilitating
tion of a duplicate of a SIM card that does not include any information or
about the victim or about their contacts; nor does it give access to applications
tions and services that have as a key recovery procedure the en-
sending an SMS, since this measure requires criminals to know

can first of all what applications the victim uses and some of the parameters

other access credentials, such as email, username,

username or password. Of course, XFERA cannot be held responsible for the

robustness in the authentication of financial institutions or services of

the information society who understand the sending of credential as safe

messages via SMS: each company must be responsible for the security

of your own measurements. Make fall on XFERA, in the form of aggravating circumstance,

the actions or omissions of third parties, is simply unconstitutional:

XFERA cannot and should not be responsible for the criminal conduct of some fraudsters.

much less from the lack of effectiveness of the authentication measures imposed.

supplemented by financial entities or other services of the society of the

information.

FIFTH.- APPLICATION TO THE CASE OF THE PRINCIPLE OF GUILT.

The aforementioned article 28 of the LRJSP also establishes the so-called "principle of

reliability", also included in article 25.1 of our Constitution. The audience

Nacional has analyzed it on multiple occasions, accustomed to quoting it in its

holdings in the following terms:

"The Constitutional Court has repeatedly declared that the principles of the order

criminal law, among which is that of guilt, are applicable, with certain

tices, to sanctioning administrative law, as both are manifestations of the

punitive action of the State (STC 18/1987, 150/1991), and that does not fit in the san-

strict or no-fault liability, by virtue of which it is excluded

and the possibility of imposing sanctions for the mere result, without accrediting a minimum

of guilt even by way of mere negligence (SSTC 76/1990 and 164/2005).

The principle of culpability, guaranteed by article 25 of the Constitution, limits the exercise of the ius puniendi of the State and requires, according to the Constitutional Court in Judgment 129/2003, of June 20, that the imposition of the sanction is based on the requirement of the subjective element of fault, to guarantee the principle of responsibility bility and the right to a sanctioning procedure with all the guarantees (STS of 1 March 2012, Rec 1298/2009).

Certainly, the principle of guilt, provided for in article 130.1 of the Law 30/1992, of November 26, on the Legal Regime of Public Administrations and the Common Administrative Procedure, provides that they can only be sanctioned for facts constituting an administrative infraction those responsible for them, even by way of simple non-compliance. Obviously, this means that this responsibility it can only be demanded by way of fraud or guilt, being banished from the scope of the law. sanctioning administrative law the so-called "strict liability", and understand- giving the guilty title recklessness, negligence or inexcusable ignorance. Is "simple non-compliance" cannot be understood, therefore, as admission to the de- sanctioning administrative law of strict liability, since the jurisprudence majority of our Supreme Court (from its sentences of 24 and 25 of January and May 9, 1983) and the doctrine of the Constitutional Court (after its STC 76/1990), highlight that the principle of guilt, even without explicit acknowledgment I quote in the Constitution, is inferred from the principles of legality and prohibition of excess (article 25.1 CE), or of the requirements inherent to a rule of law, for what is required is the existence of intent or negligence (in this sense STS of January 21 of 2011, Rec 598/2008)".

XFERA considers that this analysis should be related to the doctrine of the Tri-

Supreme Court, so many times invoked by the Agency in its resolutions, in accordance with

which “is not enough... to exculpate against a typically unlawful behavior”

I say the invocation of the absence of guilt” (STS January 23, 1998). Hence it is

Analyze below the two assumptions of which this file brings cause,

proving the absence of fault:

- In the first case, the staff of a Yoigo store was subjected to

vo of a crime of fraud, perpetrated by an individual who went to the store

exhibiting false official documentation. As stated in the Penal Code, this type

criminal is committed by those who, “for profit, use deceit bas-

enough to produce error in another, inducing him to perform an act of disposition

to their own or another's detriment”; and as expressed by the Supreme Court (sentences

of March 1, 2004, in appeal 3056/2002, and of October 9, 2005,

in appeal 86/2004):

"the concept of deception enough, can not serve to displace in the subject

liability of the crime all the concurrent circumstances displayed by the scheme

of the author of the crime, so that he ends up being responsible for the machina-

tion precisely who his victim is.”

In the case of CLAIMANT PARTY ONE, it is clear that the scammer did

everything in his power to achieve the misleading result that in effect

occurred, including the manipulation by computer programs of

Image editing of a DNI and a police report. this documentation

was kept in the XFERA systems and has been added to the file,

demonstrating that the identity verification procedure was being

actually applied by stores. cannot be derived from this

fact, therefore, no type of responsibility based on an alleged

guilt or lack of diligence, since the documentation presented appears to

ba be in order; and this has been recognized by the jurisprudence in similar cases

(Ruling of the National High Court of March 20, 2013 (rec. 581/2011,

in relation to PS/00130/2011) and Judgment of the National High Court of 29

October 2009 (rec. 797/2008, in relation to PS/00290/2008). the sentences

of March 18, 2010 (rec. 342/2009) and March 22, 2012 (rec.

9/2009) reproduce this criterion.

- The second case was the first of an operation never detected before.

hits the Masmóvil brand: the applicant had a non-activated card,

something that could only have been obtained, according to the company's procedures.

prey, after having identified himself and overcoming the security policy then

valid. Agents specialized in resolving technical incidents, such as the

who answered their call, they had no instructions to submit the applicants to the

identification procedure in cases such as the one described here, since those who

they called had outdone him by requesting the duplicate, and only they could have

received the SIM card at home, through the “***SERVI-

CIO.1”. However, in this case, the offender had obtained a

of these cards illegally, through channels outside the control of XFERA.

The company's procedures did not achieve the objective of identifying the fraud.

simply because it is a novel modus operandi: it was the first

case of these characteristics, so the risk had not been identified.

and, of course, no measures had been taken to mitigate it. As soon as

these criminal behaviors were identified by the company, adopted

all measures to detect them and react to them in the most

fast as possible, as has been shown.

In this regard, it is convenient to bring up the judgment of the Supreme Court of 1

of October 1988 (appeal 1652/1996), according to which “the guilty reproach

would have to focus, essentially, on the predictability of the given outcome.

no so"; predictability that the Agency has failed to prove in the facts of

those who bring causes this file.

SIXTH.- VIOLATION OF THE RIGHT NOT TO TESTIFY AGAINST ONESELF.

In another order of things, and in relation to the "list of 20 cases of duplicate SIM

reported/claimed as identity theft or fraudulent by customers.

tes”, XFERA understands that the actions of this Agency have entailed a violation

XFERA's right to defense, recognized in article 24 of our Constitution

tion. The request for information sent to this Agency was received only two

days after the deputy head of the management secretariat sent XFERA a

call for a meeting that took place on January 20, 2020, at

12:00 p.m., at the Agency headquarters (the email is attached, as Documentation).

to 12). The first item on the agenda of that meeting was "the duplication of cards

SIM”, and XFERA responded to the request, understanding that the requested information was

to be used within the framework of said meeting, in the context of the audit plans

preventive measures provided for in article 54 of Organic Law 3/2018 (hereinafter, LO-

PDGDD): “The Presidency of the Spanish Data Protection Agency may agree

to carry out preventive audit plans, referring to the treatments of a

specific sector of activity. Their purpose will be to analyze compliance with the

provisions of Regulation (EU) 2016/679 and of this organic law, as of

conducting research activities on entities belonging to the sector

inspected or on the persons responsible for the audit".

This belief was reinforced because the meeting was also called by the

other leading companies in the sector, that we express in it our firm will

to cooperate with the Agency to put an end to this problem, paying special attention

attention to the cases that we could identify and tightening the security measures

authority to apply; in what was an example of public-private collaboration to

try to eradicate this type of practice.

So much so, that in various meetings with the Spanish Data Protection Agency,

cough, specifically on dates, January 20, 2020, December 4, 2020 and December 18,

January 2021, which was even attended by the director of the Spanish Agency of

Data Protection, both XFERA and the rest of the operators summoned, were

proactive in the broad and extensive explanation of measures adopted and to be adopted to

control potential cases of fraudulent SIM Swapping, in the total conviction of

that the "Working Group" (so called by the Agency itself), had been conceived with

the idea of open and sincere collaboration between the parties to eradicate a practice

that, in addition, all the telecommunications operators considered foreign to them,

to the extent that all these problems are caused by a bank phishing pre-

saw and a violation of security measures of financial entities.

In the minutes of one of these meetings, drawn up by the Agency itself and provided

as Document 13, it is collected: "All of them expressed their concern about this

affair. They inform of the measures that to avoid fraud in obtaining duplicates
have been adopting lately: limit the possibilities of non-face-to-face processes,
improvements in its systems, policies and additional security protocols focused on
face-to-face processes, sanctions to distributors and commercials that do not keep
established security protocols, documentation requirements, communication channels
fraud prevention, reinforcement of audits, robotization of the process....
reported a project based on biometric recognition (requested to re-
information about these measures)".

To the extent that the Agency has the power to seek the collaboration of ad-
administered, as stated in article 52.1 of the LOPD, by virtue of which, "the Administrations
Public tions, including tax and Social Security, and individuals are-
will be obliged to provide the Spanish Data Protection Agency with the data
data, reports, background and supporting documents necessary to carry out its activity
research"; XFERA provided the information, hoping that the result of the co-
operation was the development of guidelines by the Agency, online
with the provisions of the second section of the aforementioned article 54, and not the opening of
a penalty procedure. Note that the Agency itself proposed, in
the framework of these meetings, the following (recorded in the aforementioned minutes): "Proposes the creation
creation of a common repository on good practices, for which the operations are requested
that send the measures and practices adopted to avoid cases of
fraud that they have reported and are willing to share, so that
may have a repertoire of good practices accessible to the actors involved.
two".

However, the Agency chose to use this information –provided within the framework of
the transparency and total collaboration of the telecommunications operators with the
AEPD itself, with the aim of working together to eradicate practices

illegal–as evidence in the procedure that concerns us, thus violating the guarantees

ties of the sanctioning administrative law and depriving XFERA of its right

Cho not to incriminate. Thus, it has taken advantage of a procedure of a non-sanctional nature.

such as preventive audit plans, to feed evidence into an in-

investigation aimed at exercising the sanctioning power, violating the guarantees of

everyone charged with an offence.

It is XFERA's opinion that it is not possible to exercise the power provided for in article 52.1 LO-

PDGDD regarding the company that may be the subject of an imputation in a

penalty procedure. And, of course, if the request to that administrator reaches

to take place, and the imputation finally occurs, the AEPD cannot use

no element of judgment obtained by virtue of the duty of collaboration in the framework of

sanctioning procedure, since it would imply a violation of their right to

not incriminate Indeed, the AEPD would have to use evidence that does not

were fruits of the poisoned tree, for which he would have to prove that he had obtained them.

nest with total obliviousness to the requirements of collaboration.

In this regard, it should be noted that the LOPDGDD does not establish any limitation to the

right not to incriminate oneself, so the duty to collaborate can only be understood

required with respect to third parties unrelated to the imputation that arises, or to the exercise of

powers other than sanctioning. Therefore, taking place an ultimate imputation

superior to an administrator who provided elements of judgment regarding his conduct, in

exercise of the duty of collaboration, it is concluded that it is only possible to carry out an expurgation of

the same, so that the eventual exercise of the sanctioning power is not

based on them or on any logical consequence thereof. That is, such imputation

tion should avoid being based on a fruit of the poisoned tree, understanding as such the following:

situation of violation of the right not to incriminate.

SEVENTH.- APPLICATION TO THE CASE OF THE PRINCIPLE OF SPECIALTY.

In case a total lack of guilt is not appreciated, XFERA understands that the

Agreement violates the principle of specialty that governs the sanctioning administrative law.

nador, when qualifying the facts under analysis.

In effect, the Agency qualifies those cited, on page 48 of the Agreement, as suscepti-

liable to infringe, on the one hand, "article 5.1.f) and 5.2 of the RGPD", whose sanction is recommended

ge in article 83.5.a) of the RGPD; and on the other, “of articles 25 and 32 of the RGPD”,

sanctioned in article 83.4.a) of the RGPD. Faced with the concurrence of two possible sanc-

tions for the same facts, the Agency accepts the provisions of article 29.5 of

the LRJSP, according to which "When the commission of an infraction necessarily derives-

the commission of another or others, only the corresponding sanction should be imposed.

regarding the most serious offense committed.

XFERA disagrees with this criterion, for three main reasons:

a) Article 29.5 of the LRJSP refers to what is known as “medial insolvency

of administrative infractions”, which is applicable when a more serious infraction

mild serves as a means to commit a more serious one. For it to be applicable,

it is necessary to verify the concurrence of a plurality of actions, which, in turn,

turn, give rise to a plurality of violations (for example, two events and two violations).

tions); with the particularity that one of them is a necessary instrument or means

for the perpetration of the other. In the case at hand, it is not possible to speak of plurality

of actions: there is only one action (supposedly, “not using the technical measures

and appropriate organizations to guarantee the security of the personal data of the

customers", page 41 of the Agreement), which could come to be framed, in principle, in two different offenses. As several actions do not concur, we are not facing a "con-medial course", nor can the aforementioned article 29.5 be applied to the case.

b) In both alleged infractions, the unlawful conduct would be the same: the insufficiency science of the technical and organizational measures applied by XFERA; and the disrespect imputed in both is also the same, consisting of the presumed noncompliance ment of the duty to protect customer information. Qualify the same he-chos, with the same author and the same foundation, as two infractions supposes in-occur in duplicity, which is contrary to law, by violating the principle non bis in idem. Such principle is enshrined in article 31.1 of the LRJSP, which provides that "the facts that have been criminal or administrative may not be sanctioned positively, in cases in which the identity of the subject, fact and foundation can be appreciated". In short, the factual basis of the imputed infringement is coincident, and the foundation to punish her as well. The only difference between the two offenses charged indicates that, in serious cases, the sanctioned conduct consists of the failure to adopt those technical and organizational measures that are appropriate to guarantee a level of security appropriate to the risk of the treatment; and in the very serious, the conduct sanctioned consists of violating the principle of the RGPD from which the need arises to adopt such measures.

c) In the present case, we are facing what the doctrine calls "apparent competition of laws". This is a figure analyzed on multiple occasions by the Supreme Court.

premo, which defines it as follows in its judgment of May 22, 2009 (rec.
10084/2008): "The so-called conflict or contest of norms occurs when on a
same assumption of fact fall two or more normative precepts in whose respective
two hypotheses is entirely subsumable the assumption in conflict (...) The conflict of
rules -in effect- must be resolved with the application of only one of them, which excludes
to the others (which is why some speak of an apparent conflict, since it ultimately
disappears in favor of a single norm)". On which of the norms to apply in ta-
situations, the Supreme Court clarified it in a judgment of September 22,
2011 (appeal 4289/2009), saying that "in case of conflict, the rule that adjusts
more exactly to the assumption of fact expresses in a more complex way the valuation
that of the same makes the legal system and prevails over the one that contemplates it
more vaguely and abstractly. In this regard, given that the specific infringement is the
serious, it is concluded that, in the worst case scenario for XFERA, the sanctioning resolution
could only declare the serious infringement.

EIGHTH.- APPLICABLE CIRCUMSTANCES TO THE INDIVIDUAL CASE, ACCORDING
TO ART. 83.2 GDPR.

If a total lack of guilt is not appreciated, it cannot be ignored that the conviction
conduct deployed is less serious than that considered in the Agreement:

8.1) ABOUT THE "EVIDENCE FOR A POSSIBLE GRADUATION FROM THE
AMOUNT OF THE SANCTION".

The Report of Previous Investigation Actions includes, in its Annex I (page
pages 13 and 14) a series of criteria that are listed in order to graduate the position
possible sanction to be imposed on XFERA. On this list, it is convenient to make a series
of nuances:

 In relation to the continuing nature of the facts verified,
reflects that "the entity declares 44 cases detected annually (2019)".

After reviewing this data internally, it has been concluded that ten of the

those initially declared were intrusion tests carried out by the

security personnel of the company, with fictitious data, for the purposes of

evaluate the robustness of the then existing procedures, in the

framework of the implementation of the new security layers implemented

mentioned, and which are described in section 2.1. of the present

cations. Therefore, the figure must be reduced to ***AMOUNT.6.

It is noteworthy, on the other hand, that the Start Agreement (page 46)

increases the amount to ***QUANTITY.7, we understand that due to al-

some mistake It is insisted that the correct number is ***QUANTITY.6.

 Despite the fact that the Report of Previous Actions acknowledges that “there is no

It is known that procedures have been resolved for infractions from

of the same facts by the investigated entity”, the Agreement

Home does not take this mitigating circumstance into account.

8.2) ABOUT THE GRADUATION CRITERIA EFFECTIVELY RECOGNIZED

GIDOS IN THE AGREEMENT.

On pages 45 and following, the Agreement analyzes the alleged circumstances

aggravating and mitigating circumstances applicable to the case. About:

 On the "nature, seriousness and duration of the infraction", the Agency

understands that its nature is very serious, because it entails "a loss

disposition and control over personal data”. XFERA disagrees with

this statement, because:

o What is produced is a duplicate of a SIM card, which is not

of personal data: a SIM card is a device that does not

contains personal information of any kind; Y

o The loss of disposal and control over the data occurs

on third-party platforms, which employ SMS messages

as an authentication method, even knowing its manifestation.

your lack of security.

As stated, the administrative responsibility derived from the

lack of diligence of the owners of said platforms cannot be

attributed to XFERA.

 In the same section, and in terms of duration, the Agency states

that the facts cover "a period of more than 9 months", since the

“last of the cases not presented before this Agency” occurred on 12

April 2020. As has been proven, this specific case was detected

ted by the successive security layers implemented by XFERA,

and did not give rise to any fraud. For these purposes, the dates to be taken into

account should be:

o On November 28, 2019, the date on which the

new security measures by Masmóvil, which works

tion with a cumulative efficacy of ***PERCENTAGE.9; and his-

put an effective reduction of ***PERCENTAGE.10 in the

sos in which criminals achieved their illicit objectives; either

failing that

o On January 20, 2020, the date of the last of the pending cases

in the file in which fraud was confirmed;

 Number of interested parties affected: as has been said, the number of

detected in 2019 was ***QUANTITY.6, and not

***QUANTITY.7, as indicated in the Agreement. This number was reduced to 3 in

2020, having in that year XFERA almost 7.2 million mobile lines,

as a result of the application of the new security measures

by XFERA;

 Level of damages and losses suffered: the Agency considers them serious.

You see, but XFERA disagrees with this statement. The only damage suffered

two are derived from the cost of duplicating the SIM card (€6 +

VAT), which have been returned to all those affected who have claimed them.

mado. Bank fraud covered by the Agreement is not the responsibility

of XFERA, but of the financial entities that use SMS as

authentication measure, even knowing its lack of security.

Holding XFERA administratively responsible means bankruptcy

inadmissible principle of personality, contained in article 28 of

the LRJSP and in article 25.1 of the Constitution;

 Alleged negligence of XFERA: it could not be accredited by the

Agency. The XFERA staff was deceived by criminals, and pre-

submitting their lack of diligence supposes violating the doctrine of the High Court

National, according to which "no guilt can be assessed (not even

by way of fault or lack of diligence) in the actions of the re-

current, that he acted in the belief that the person with whom he contradicted

taba was who he claimed to be and identified himself as such with documentation

appearance authentic and corresponding to it";

 Degree of responsibility: the Agency estimates that it is "high", but it does not justify

This explains why, despite the fact that article 83.2.d) RGPD establishes that

must be put in relation to "the technical or organizational measures that

have been applied by virtue of articles 25 and 32" of the same norm.

It has been proven that there were reasonable security procedures

in relation to the foreseeable risk for the company in the mo-

ment of the facts; and that subsequently, the security procedures

security have been extraordinarily reinforced, with outstanding results.

outgoing. Understand as "high" the degree of responsibility, in view

from the above, it lacks all logic;

 Categories of personal data affected: it is surprising that the Agency

consider that a SIM card is a category of personal data

whose unauthorized access is "particularly serious". SIM cards

They are not personal data: they are mere supports, and when accessed

activates a duplicate, they are empty of content. The truth and truth is that

There is no category of personal data affected by this operation.

tive, as far as mobile phone operators are concerned.

8.3) ON THE DISPROPORTION OF THE AMOUNT OF THE SANCTION PRO-

PUT.

It should be noted that, if a total lack of guilt is not found, in

In any case, a qualified decrease in culpability should be appreciated.

nature of XFERA or, at least, of the unlawfulness of the facts of which
the present procedure brings cause, which would determine the origin of re-
reduce the seriousness of the infractions attributed to it and, therefore, to reduce the
penalty to be imposed. Indeed, considering the previous arguments of culpability
even if they were not estimated, it could not be ignored that, due to the circumstances
concurrent conditions, the behavior displayed is less serious than the
determined by the Agreement. Taking into account, furthermore, that almost all of the
the aggravating circumstances included therein are not applicable to the case,
It is concluded that it is only possible to reduce the sanctions that are eventually imposed
won Especially when the effort made by XFERA to adapt its products
security procedures to the new reality derived from “SIM swapping” is
more than remarkable, and its results, exceptional.

FIFTEENTH: On May 5, 2021, the instructor of the procedure
agrees to open a period of practice tests, which is notified to XFERA,
on May 5, 2021, in the following terms:

"1. The international claims are considered reproduced for evidentiary purposes.
put by A.A.A., E.E.E. and its documentation. Also, the documents
obtained and generated by the Inspection Services before XFERA MÓVI-
LES, S.A, and the Report on previous actions of the Subdirectorate General
of Data Inspection that are part of file E/11418/2019.

2. Likewise, they are considered reproduced for evidentiary purposes, the allegations
to the initiation agreement PS/00027/2021 presented by XFERA MÓVILES,
S.A. on March 8, 2021 through the General Registry of this

Agency, and the documentation that accompanies them:

Doc. 1. Official letter of the Investigating Court No. 9 of Alicante

Doc. 2. SEAD requirement

Doc. 3. Data protection impact assessment

Doc. 4. Risk analysis

Doc. 5. SIM change protocol

Doc. 6. Duplicate SIM table

Doc. 7. Audio file: ***TELEPHONE.4

Doc. 8. Audio file: ***TELEPHONE.7

Doc. 9. Audio file: ***TELEPHONE.10

Doc. 10. Audio file: ***TELEPHONE.13

Doc. 11. Audio file: ***TELEPHONE.19

Doc. 12. AEPD call

Doc. 13. AEPD Minutes”

SIXTEENTH: On October 4, 2021, the instructor of the procedure

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

XFERA MÓVILES, S.A., with NIF A82528548, 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 250,000'00 (two hundred and fifty thousand euros).

ros).

On October 4, 2021, through the Electronic Notification Service and

Electronic Address Enabled, the Resolution Proposal is notified.

SEVENTEENTH: On October 8, 2021, XFERA requests the extension of the

term to formulate allegations to the Resolution Proposal.

EIGHTEENTH: On October 13, 2021, the Agency grants the extension

tion urged.

NINETEENTH: On October 26, 2021, XFERA makes allegations to

the Resolution Proposal, in which it states, in summary, the following:

FIRST. Disagreement with the qualification of the alleged infraction.

It alleges that the AEPD made an incorrect qualification of the assumption of fact, derived

of an inadequate interpretation of the so-called "specialty principle".

XFERA recalls that in the Agreement to Initiate the procedure, the Agency qualified the

facts as likely to infringe, on the one hand, "article 5.1.f) and 5.2 of the RGPD",

whose sanction is included in article 83.5.a) of the RGPD; and on the other, “of articles 25

and 32 of the RGPD", sanctioned in article 83.4.a) of the RGPD. And that before the concurrence-

ence of two possible sanctions for the same facts, the Agency argued the provisions of

Article 29.5 of the LRJSP: "When the commission of an infraction necessarily derives

seriously the commission of another or others, only the corresponding sanction should be imposed.

regarding the most serious offense committed.

The aforementioned legal qualification was, in XFERA's opinion, contrary to law, and

This was reflected in the pleadings brief to the Initiation Agreement of this proceeding.

penalty, mainly for three reasons:

1. Because article 29.5 of the LRJSP refers to the medial infraction contest-

administrative purposes, for which it is necessary to verify the concurrence

of a plurality of actions that, in turn, give rise to a plurality of in-

fractions; with the particularity that one of them is an instrument or means

necessary for the perpetration of the other. Something that does not happen in this case,

in which a single action occurs;

2. Because both the facts, as well as the unlawful conduct and the imputed disrespect

by both offenses would be the same, which would violate the principle

"non bis in idem"; Y

3. Because we really find ourselves before an "apparent contest of laws", and such

course must be resolved with the application of only one of them, which must be

the one that most closely matches the factual assumption. This maxim is

known by the doctrine as "principle of specialty of administrative law

you sanctioner".

XFERA alleges that the resolution proposal partially accepts this allegation, but

it does so by redirecting the imputation of the infractions initially considered to

a single infraction, derived from the violation of article 5.1.f) of the RGPD. And what is

this renewal which, in the opinion of XFERA, continues to violate the aforementioned principle

specialty pio, as will be explained below.

The figure of the apparent competition of laws was analyzed on multiple occasions by the

Supreme Court, which defines it as follows in its ruling of May 22, 2009

(rec. 10084/2008):

“The so-called conflict or contest of norms occurs when, on the same subject,

In fact, two or more normative precepts fall into whose respective hypotheses

sis is entirely subsumable the assumption in conflict (...) The conflict of norms -in

effect- must be resolved with the application of only one of them, which excludes the other

more (which is why some speak of apparent conflict, since this finally

disappears in favor of a single norm).

On which of the norms to apply in such situations, the Supreme Court clarified it in

Judgment of September 22, 2011 (appeal 4289/2009), in the following terms:

us:

“This conflict of laws must be resolved through the application of the generic principle

specialty, which is broken down into a series of rules that, as is known, in the

currently contained in art. 8 CP, and that respond to the same idea, namely:

that in the event of a conflict, the rule that most closely matches the assumption

In fact, it expresses in a more complex way the valuation that the order makes of it.

legal system and prevails over the one that contemplates it in a more vague and abstract way.

tract. (…)

It should be clarified that the circumstance that such rules are contained in a precept

of the CP and that the LGT does not make an express reference to it does not imply, however,

However, they should not be used in the scope of the sanctioning administrative procedure.

nador, given that the aforementioned art. 8 of the CP does not come more than to collect criteria of inter-

interpretation to determine the applicable Law or legal precept that had already been assumed.

measured by criminal doctrine and applied by the jurisprudence of the Supreme Court

mo".

Well, XFERA understands that the instructor errs by subsuming behaviors, not in

the most exact and concrete article, but in that other more vague and abstract, violating

thus the doctrine of the Supreme Court. Specifically, it qualifies the behavior as "the treatment

processing of personal data violating the principles and guarantees established in the

Article 5 of Regulation (EU) 2016/679", when the LOPDGDD typifies another conduct

that fits much more exactly to the assumption of fact, in his opinion, which

is "the lack of adoption of those technical and organizational measures that result

appropriate to guarantee a level of security appropriate to the risk of the treatment,

in the terms required by article 32.1 of Regulation (EU) 2016/679".

In addition, XFERA understands that, in the present case, the Agency itself recognizes in

multiple occasions that the reason for the sanction is not the absence of safety measures.

security, but its supposed insufficiency. This is expressed, for example, on page 84

of the motion for a resolution, where it is stated that:

"Thus, the infraction becomes not due to the lack of a specific security policy

for the issuance of SIM duplicates, but because of the need to review and re-

force".

Moreover, on page 79 of the proposal, the intention of the Agency is verbalized with the sanction:

“In this sense, this Agency wants to reinforce the need to improve this first security layer that is what gives access to the fraudulent obtaining of a duplicate of a SIM card by criminals”.

XFERA considers that if both the LOPDGDD and the Regulations themselves include a specific infraction derived from the breach of article 32 of this last rule, it is because the legislator's intention was that security breaches ity have their own typification. And that by not applying it in the present case, the Agency departs from the spirit of the rule, empties article 73.f) of the LOPDGDD and ignores the specialty principle applicable to administrative law sanctioning, thus departing from the consolidated doctrine of the Supreme Court.

In the same way, XFERA understands that the Agency incurs in a clear inconsistency with their own acts and, specifically, with previous procedures in which the en- responsible entities would not have adopted adequate security measures, and sanctions them (correctly applying the principle of specialty, and despite the great truth of the facts) for breach of article 32 of the RGPD, and not of article 5.

They cite, for example:

Yo.

ii.

PS/00362/2021, where BBVA is sanctioned because "the entity claims da facilitates the detail of the last movements of the Affinity Card me- through an automated telephone service system on the phone ***TELÉ- FONO.1 in which only the client's DNI is requested as identification data. te”, and the sanction is based on “the alleged violation of article 32 of the RGPD,

typified in article 83.4.a) of the RGPD"; Y

PS/00179/2020, where Air Europa is sanctioned because a "hacker committed

promised a series of systems" of the company, having confirmed "that the

attacker had collected 488847 unique credit cards" from his customers; Y

the sanction is based again on "an infringement of article 32.1 of the RGPD, typi-

ified in Article 83.4.a) of the RGPD".

XFERA alleges that, despite having raised this argument in the allegations

raised against the Initiation Agreement, this Agency has not clarified the reason why

which has decided to qualify the conduct as an infringement of article 5 of the RGPD, and not of the

article 32. And that this is sufficient cause to speak not only of a clear inconsistency

omission (for failing to comply with the duty to state the reasons provided for in art.

article 89.3 of Law 39/2015), but also of an arbitrary action, proscribed by

Article 9.3 of the Constitution, in which there is evidence of discriminatory treatment with

others managed.

Taking into account the foregoing, XFERA understands that the qualification of the conduct must-

could be based, also in this case, on the infringement of the provisions of article 32

of the RGPD, typified in article 83.4.a) of the aforementioned Regulation, and qualified as

serious for prescription purposes in article 73.f) of the LOPDGDD. And that, in the mean-

day in which, in the Home Agreement, the administrative fine for

this cause in €100,000, such should be the maximum amount of the sanction to be imposed.

SECOND. XFERA has not broken the principle of data confidentiality.

As reflected in the Legal Basis (hereinafter, FD) fifth of the Pro-

resolution, “this Agency considers that, in both cases, what is being

analyzing is the violation of the principle of confidentiality of the data by having carried out

do the duplication of the SIM card without having the adequate security measures”.

It is also stated that "both the data that is processed to issue a duplicate card-

ta SIM as the SIM (Subscriber Identity Module) card that uniquely identifies

univocally and univocally to the subscriber on the network, they are personal data, and their tra-

treatment be subject to data protection regulations.

XFERA understands that the Agency is wrong in making both statements.

Since personal data is defined as “any information about a natural person

identified or identifiable” (bold is from XFERA). XFERA alleges that, by definition,

both data and information are intangible resources, so it is unacceptable

It is not possible for a “SIM card”, which is a physical object, to be considered by this Agency

as "personal data". It is not, nor are a mobile phone, a computer,

a USB memory or a credit card: all of them are mere supports; and he-

In fact, its nature fully fits the definition of "support" offered by the

Royal Decree 1720/2007, of December 21, which developed the old LOPD: “Ob-

physical object that stores or contains data or documents, or object that can be

treated in an information system and on which data can be recorded and retrieved.

cough".

XFERA argues that a SIM card is a physical object, which, as recognized by the

Resolution Proposal, (1) it is capable of storing data, (2) it can be used

done in information systems, by means of a mobile phone and (3) allows recording and

retrieve information; and in fact, the proposal states, on page 72, that “the card

This SIM constitutes the physical support through which the character data is accessed.

staff".

And he alleges that the contradiction incurred by the Agency itself is evident.

Based on the foregoing, XFERA alleges that, as has been highlighted in the allegations,

tions made to the Start Agreement, the SIM card that is given to the user when making

a duplicate is blank, i.e. it does not yet contain personal data

of any kind. And that, contrary to what the Agency affirms in its resolution, the

MSISDN (ie the user's phone number) is not stored on the SIM card.

XFERA recalls that information has been provided to the file, published by the

national regulator on the matter (the CNMC) in which it is expressed, black on white and

literally, that “our phone number is not stored on the SIM card

MSISDN”; but despite this, and persisting in its error, the Agency insists on affirming

that this type of card “contain[s] a chip in which the MSISDN is stored” and that

“the SIM card identifies a phone number”. XFERA considers that these affirmations

nes are simply unrealistic.

XFERA alleges that the SIM card only includes cryptographic keys and a number

number, called IMSI, which does not refer to any person: it only identifies

to the card itself. And that what is commonly known as "activate a SIM card"

is a technical procedure that XFERA carries out on its own servers, consisting

in deriving the traffic generated or directed to an MSISDN to the IMSI of said SIM card.

XERA considers that there is no doubt that carrying out this procedure "supposes

the processing of personal data” of the owner of the telephone line; but this deal

The processing is carried out on the XFERA servers, never on the SIM card itself, whose

content remains unchanged and, therefore, empty of all personal data.

XFERA points out that, in relation to the IMSI included in the duplicate card, in no

moment it is used in the mobile phone of the owner of the line, so it is not

possible to associate it with this person: in any case, it could come to be associated with the

offender who makes the illicit duplicate of the aforementioned card, but every time his identity

entity is unknown, we would not be dealing with personal data.

XFERA also draws attention to the fact that, in the Resolution Proposal, it is made

reference to the IMEI, since it is a code that uniquely identifies a

specific mobile phone terminal, that is, to the device itself, to the mobile phone in

Strict sense; and it has nothing to do with the SIM card or the IMSI. In the case that

we are dealing with, the IMEI would again be that of the offender's phone, since it is

We are talking about the duplication of SIM cards, not the cloning of mobile phones; and

We insist that his identity is unknown. Hence, XFERA understands that lack

It makes sense to use it to justify the existence of personal data processing.

beyond the fact that the instructor may have been confused by the profusion of acronyms

We are used in the sector.

In short, XFERA alleges that the user who obtains a duplicate of a SIM card

receives a blank support, which does not contain any information. The personal data

those of the owner of the line remain, at all times, guarded on the servers

of XFERA, so access to a copy of the SIM card does not imply any kind of

of loss of disposal or control over such data. Therefore, in the opinion of XFE-

RA, in the present case there is no violation of the confidentiality of the data.

cough of those affected in the treatment consisting of the duplication of the SIM card, and

Not a single piece of evidence has been adduced in this proceeding to contradict this assertion.

tion.

THIRD. Violation of the principles of personality of the sanction and typicity.

XFERA highlights the following from the Resolution Proposal:

“In this regard, this Agency recalls that in order to complete the scam object of the «SIM swap-

pping”, it is necessary for a third party to “impersonate the identity” of the owner of the data before

the financial institution. What entails a priori, a treatment outside the principle of

legality because a third party is processing data, since it has access to them, without legal basis

any, in addition to the violation of other principles such as confidentiality.”

And he states that "it escapes all logic" that, being aware of this authority of con-

control that the offender and the financial institution are the subjects responsible for the

unlawful conduct that is intended to eradicate (which is "avoid this type of scam",

according to the Resolution Proposal), this file is directed solely against this

communications company. And he points out that, in colloquial language, instead of directing-

I know the origin of the problem, it seems that this Agency chooses to "attack the messenger";

something that, as has been stated in previous allegations, is contrary to the principle of

personality of the sanction, foreseen in article 25.1 of our Constitution. It tra-

of one of the pillars of the punitive law of the State, which entails “the impossibility

of the transfer of the sanctioning consequences on persons or entities dis-

inks of the authors of the punishable acts”, in the words of the National Court,

which cites the doctrine of our Constitutional Court on the matter as follows:

“The Sentence of the Constitutional Court 219/1988, of December 22, proclaimed

that the principle of personality of sanctions or of personal responsibility for

own facts prevents an undue transfer of punitive responsibility to a person

unrelated to the infringing act, since this would entail accepting a liability regime

objective that would violate the requirement of intent or negligence necessary for the existence of

administrative infraction".1

XFERA argues that, in the present case, the Agency anchors the responsibility of the con-

conduct in which, by providing XFERA duplicate SIMs to third parties other than the holder

of the line, unauthorized access is granted to the personal data of those affected.

two, and therefore the elements are given to attribute responsibility to my client.

However, XFERA understands that this approach is contrary to law, for

three reasons:

1. In the first place because, as has been stated, the SIM accessed by the offender

account is empty of all content. The criminal does not access any data

victim's personal information during the process of duplicating the card, because all

Both the customer data processing necessary to activate the card are

carried out exclusively on XFERA servers, which are not violently

two in this operation. And XFERA understands that at no time has it achieved

show this Agency that there has been, in this procedure, access

not authorized to personal data that are subject to treatment by XFERA;

2. Secondly, because the SIM duplication only gives access to the de-

linked to the victim's telephone line, and through it, to the content of

the messages that can be sent and received. Nevertheless:

a. The activity of XFERA, in relation to said messages, is of mere

intermediation in data transmission. Therefore, it cannot be considered

hold XFERA responsible neither for transmitting nor for facilitating access to di-

this information, since it is exempt from any responsibility in this regard,

in accordance with article 14.1 of the LSSI, which reads:

"Telecommunications network operators and service providers

access to a telecommunications network providing an internet service

mediation consisting of transmitting over a telecommunications network

data provided by the recipient of the service or to facilitate access to

They will not be responsible for the information transmitted, unless

they themselves originated the transmission, modified the data or

selected these or the recipients of said data."

b. Additionally, such access does not imply a violation of the right

to data protection, but, in any case, to another fundamental right

such closely related, but autonomous and independent: the secret of the

communications, whose tutelage is beyond the scope of competence of this

Agency; Y

3. Thirdly, because although, through the messages received, the offender

account could access personal data of the victim, XFERA cannot be

held responsible for such acts. Although it is undeniable that, after

record the duplicate of the card, the offender can achieve "control of the

SMS addressed to the phone linked to the initial SIM card" (page 74 of the pro-

put), it is also true that XFERA is not "responsible" or "in charge" of any

any of the treatments to which the offender manages to access independently

via said SMS: it is a mere "third party", in accordance with article 4 of the

GDPR; and third parties are not subject to the sanctioning regime provided for in the

Regulation itself or in the LOPD.

In this regard, XFERA alleges that recital 74 of the RGPD, invoked by this Agency in the Resolution Proposal, it is clear when it states that “It must be established the responsibility of the person in charge of the treatment for any treatment of personal data made by himself or on his behalf” (bold is XFERA).

This is not the case, therefore, in XFERA's opinion, in accordance with the principle of typicity, the conduct of XFERA cannot be sanctioned, in relation to said treatments.

XFERA argues that, ultimately, the only argument put forward by this Agency (p. 83) is that "if access to SIM cards by parof these criminals, they could not benefit from the possibilities offered by the online banking to get your benefit. And that it is an assessment based on mere supositions that make it obvious that the same objective would be achieved if online banking stopped of using SMS, a manifestly and inherently insecure method, to send credence. authentication credentials to your customers; or if instead of sending the keys themselves authentication as part of the messages, ask more robust questions, such as this operator is suggested on page 76 of the Proposed Resolution. All this, for the rest, in line with what was resolved by the courts in similar cases: without going any further far away, this is how the Supreme Court (Second Chamber) has analyzed it in its recent ruling of February 12, 2020 (appeal 10,169/2019), which attributes responsibility in these assumptions to banking entities:

“In cases like the present one, it is clear that the activity proposed by the banking entity ria to its clients through online operations presents some risks derived from the possibility of impersonation of the identity of the person who contracts with the entity for the carrying out operations without the authorization of the authentic contracting party. It is also clear Also, excluding willful misconduct or gross negligence on the part of the customers, the bank is responsible for offering and implementing a system

safe, so that the negative consequences of failures in it do not de-

must be transferred to the client".

XFERA understands that the Supreme Court's position is clear: it is the bank, and not the company

of telecommunications, the "responsible for offering and putting into practice a se-

guro"; and at no time has XFERA been contracted (or even contacted) by the

financial institutions to secure their systems, so it makes no sense to blame

XFERA for the negative consequences derived from the weakness of the augmentation method.

chosen temptation. A weakness that the Agency itself acknowledges on its own site

website, in which he recommends users, literally: "Avoid SMS as a method

two-step authentication."2

What is certain and true, continues XFERA, is that the banking entities opted for

var authentication via SMS without counting at any time with the opinion of the

telecommunications operators, and without considering that their obligations in terms of

are not only those dictated by the PSD2 Directive, but also those

imposed by the GDPR. And considers that punishing XFERA for the irresponsibility

of banking, therefore, is not only materially unfair, but also lacks support

normative.

QUARTER. Violation of the principle of culpability.

4.1. XFERA had not identified the risk, simply because it did not exist before

PSD2.

XFERA cites the RGPD, in its article 32, which establishes: "the person in charge and the person in charge

of the treatment will apply appropriate technical and organizational measures to guarantee
a level of security appropriate to the risk. And remember that, regarding the concept of
“risk”, this Agency analyzes it in its “Practical Guide to risk analysis in trades”.
processing of personal data subject to the RGPD”, on page 5 of which the following is collected:
following:
“A risk can be defined as the combination of the possibility of the materiali-
ce a threat and its negative consequences. The level of risk is measured by your
probability of materializing and the impact it has if it does. the threats-
hazards and the associated risks are directly related: consequently, identi-
Identifying risks always implies considering the threat that can cause them.”
XFERA alleges that, in the present case, the threat that originated the risk that brings
cause this file was born in 2019, with the entry into force of a regulation (the Di-
Directive (EU) 2015/2366, or PSD2) that began to be applied on September 14, 2015
cho year. Until then, financial institutions did not use SMS as a double
authentication factor, so there were no cases of fraudulent duplication of
SIM cards to commit fraud.
Given that the identification of the risk implies considering the threat that can originate it,
nar, and given that the threat did not exist prior to the application of
the PSD2 Directive, understands that it was impossible for XFERA to have identified said
risk. This was stated in the pleadings brief, indicating that XFERA had no
effective knowledge of this problem until September 26, 2019, when
do receives a request from the General Subdirectorate of Attention to the User of Tele-
communications, of the Secretary of State for Digital Advance.
Given this news, XFERA reinforced the identification procedures and activated
two additional layers of security, which began to be applied on November 28
2019. All this, in line with what is recommended by the Agency in the aforementioned Guide:

“Guaranteeing adequate risk management requires continuous monitoring of

the risks and periodic evaluation of the effectiveness of the control measures defined

taken to reduce the level of risk exposure.

It is recommended to review the risk analysis carried out in the event of any significant change.

tive in treatment activities that may lead to the appearance of new

risks”.

It is alleged that this was exactly what XFERA did; and despite complying with

recommended by this Agency, however, it is sanctioned, based on a kind of

Strict liability derived from its condition as "depository of data of a

large-scale staff. Unfortunately, and contrary to what this

control authority, argues XFERA that large companies do not have the skills

divinatory, especially when the risk arises from the way in which certain

financial institutions applied a new regulation, without counting on the operators

telecommunications radios.

And he states that he finds the following excerpt from the

Resolution Proposal (page 84):

“That is to say, from the point of view of culpability, we are facing a defeatable error, since

with the application of the appropriate technical and organizational measures, these supplant-

tions of identity could have been avoided. Especially when XFERA admits in its

allegations that before September 26, 2019 I had not even identified

the risk".

XFERA indicates that it is surprising because, in the present case, it is not about
that XFERA had not identified a previously existing risk, due to lack of care.
given in the analysis of the threats that could materialize. On the contrary,
It is a risk that, directly, did not exist. And he wonders: how does it fit, then,
call it a "beatable error"? XFERA goes on to say that the Agency itself recognizes
ce that he had no news of this operation until (page 5):
“Dated November 27, 2019, the director of the AEPD, before the news appeared-
in the media regarding the use of fraudulent practices
based on the generation of duplicate SIM cards without the consent of their
legitimate owners in order to access confidential information for criminal purposes
(known as “SIM Swapping”), urges the Subdirectorate General for Inspection of
Data (hereinafter, SGID) to initiate ex officio the Preliminary Investigation Actions
tion aimed at analyzing these practices and the existing security measures to
its prevention”.
And that, by the time the director of the AEPD learned of the existence of the practice co-
Known as SIM swapping, XFERA had already reacted, by developing
its new security system Alerta FSM, which was implemented that same week.
na, with magnificent results. And despite the significant and rapid improvement in its
security measures, which the Agency itself praises, XFERA is forced to pay
a very important sanction, which grossly violates the principle of culpability
enshrined in articles 28 of the LRJSP, and 25.1 of the Constitution. How do I recognize
The Supreme Court ruled in its judgment of October 1, 1988 (appeal
1652/1996), “the guilty reproach would have to focus, essentially, on the pre-

visibility of the harmful result"; predictability that, in XFERA's opinion, the Agency has not been able to prove the facts of which this file brings cause.

4.2. XFERA acted in the belief that the person requesting the duplicate was who he claimed to be.

XFERA recalls that the entity's staff was the passive subject of a crime of misrepresentation. documentary quality in medial competition with another fraud, perpetrated by criminals who go to their establishments displaying false official documentation. And that, as stated in the Penal Code, the type of fraud is committed by those who, "with the intention of for profit, use deception enough to produce error in another, inducing him to realize carry out an act of disposition to the detriment of oneself or another"; and as stated by the Court Supreme Court (judgments of March 1, 2004, in appeal 3056/2002, and of October 9, 2005, in appeal 86/2004):

"the concept of deception enough, can not serve to displace in the passive subject of the crime all the concurrent circumstances displayed by the trick of the author of the crime, so that he ends up being responsible for the machination precisely who is his victim?

XFERA cites as an example the case of Mr. Torrado, where, in its opinion, it is evident that the scammer went to great lengths to achieve the misleading result that actually occurred, including manipulation by computer programs Image editing costs of a DNI and a police report. this documentation was kept in the XFERA systems and has been added to the file, showing finding that the identity verification procedure was being effectively applied by stores. XFERA considers that it cannot be derived from this fact, therefore, no type of responsibility based on an alleged culpability

diligence or lack of diligence, since the documentation presented appeared to be in order;

and this has been recognized by the jurisprudence in similar cases, of which are provided

as an example the following:

Yo. Judgment of the National Court of March 20, 2013 (rec. 581/2011, in rela-

with PS/00130/2011): "The Chamber considers that on those two contracts of the same

same name on which there is evidence, albeit a posteriori, of all the supporting documents

additional, there is no lack of diligence, in the sense required in art. 130.1 LRJyPAC, al

include the documents that accredited the alleged unequivocal consent, which

they were subsequently revealed to be fraudulent".

ii. Judgment of the National Court of October 29, 2009 (rec. 797/2008, in re-

relationship with PS/00290/2008): "For all of which and in view of the special circumstances

concurrent instances in the case at hand, no guilt can be assessed (or even

want by way of fault or lack of diligence) in the actions of the appellant entity,

that he acted in the belief that the person he was contracting with was who he claimed to be

and was identified as such with an apparently authentic documentation and with it

corresponding, for which it was legitimated to process its data of character.

be personal". The judgments of March 18, 2010 (rec. 342/2009) and March 22,

zo of 2012 (rec. 9/2009) reproduce this criterion.

XFERA argues that it is undeniable that, as the Agency affirms, the security measures

implemented failed to prevent duplication of SIM cards; but also

It is that if the measures did not achieve their objective, it was because the criminals

They managed to deceive the XFERA staff, exceeding the established procedures
through false documentation; and that when this new operation is detected, XFERA re-
forced these security measures, managing to detect and block the vast majority
of fraud attempts perpetrated by criminals.

On the other hand, XFERA cites the Resolution Proposal (page 76):

“Although this Agency recognizes the improvement produced in the procedures implemented
two, it is still striking that in the face-to-face channel elements were not reviewed
data from the DNI itself that could give clues as to whether it was an original document
or a fake. Nor has it been found that training or material was given
in this regard to the agents in charge of this task, who are the ones who carry out this
verification of the identity of the person.

In this regard, XFERA alleges that it provided training to workers on the commitment
bation of the security elements of DNI and passport, since it is part of the course
they receive when they start working in the company. And that, as can be seen in
the material that is attached as Document 1 of these allegations, the information
The training is exhaustive and includes the most used types of identification documents.
two in Spain. XFERA mentions that this information remained published in the
"Commercial Portal" of the company, available for consultation by the staff in any
any moment And that if it was not provided at an earlier time, it is because the Agency,
he just didn't ask for it; therefore, it is requested that it be taken into account for the purposes
opportune cough.

The Agency also affirms that “there is no question that XFERA agents did not comply with
plied with the established procedures, but rather that the measures taken
Views were not adequate. However, XFERA highlights that the standard does not require the ab-
solute effectiveness of the security measures, but that they are "appropriate to guarantee
guarantee a level of security appropriate to the risk” (article 32 of the RGPD), and, in his opinion,

ion, the AEPD has not been able to demonstrate that lack of adaptation to the known risk,

with the information available at the time the events of the

that brings cause this procedure.

FIFTH. Circumstances applicable to the individual case, in accordance with art. 83.2 GDPR.

On pages 99 and following, the Motion for a Resolution analyzes the alleged cir-

aggravating and mitigating circumstances applicable to the case. In this regard, XFERA points out:

~

Regarding the nature, seriousness and duration of the infraction, the Agency understands

that its nature is very serious, because it entails "a loss of disposition and

control over personal data. XFERA disagrees with this statement, because

as already stated:

What is produced is a duplicate of a SIM card, which does not contain

personal data: a SIM card is a device that does not contain information

personal training of any kind; Y

The loss of provision and control over the data occurs in platforms

forms of third parties, which use SMS messages as a method of

authentication, even knowing its manifest lack of security.

XFERA understands that the administrative responsibility derived from the

lack of diligence of the owners of said platforms cannot be

attributed to XFERA, because it only holds the position of "third"

in relation to these treatments.

~

Regarding the level of damages suffered: the Agency considers them high,

but XFERA disagrees with this statement. Understand that the only damage suffered

two are derived from the cost of duplicating the SIM card (€6 + VAT),

that have been returned to all those affected who have claimed them. alleges

that the bank fraud included in the Agreement is not the responsibility of XFE-

RA, but of the financial entities that use SMS as an autho-

attempt, even knowing its lack of security. And what to hold

administratively to XFERA supposes an inadmissible breach of the principle of

personality, collected in article 28 of the LRJSP and in article 25.1 of the

Constitution.

~

. On the alleged negligence of XFERA: XFERA understands that it has not been able

be accredited by the Agency. And that the XFERA staff was deceived by

offenders, and presume their lack of diligence is to violate the doctrine of the

National High Court, according to which "no guilt can be assessed (not even

whatever by way of fault or lack of diligence) in the actions of the entity

rrente, who acted in the belief that the person he was contracting with was

who claimed to be and identified himself as such with documentation that appeared to be

authentic and corresponding to it".

The AEPD points out that "it is proven in the file that it has not been guaranteed

adequate security in the processing of personal data, enabled

gives an account of the result that identity theft has produced." Understand-

of XFERA that this statement is close to the figure of objective responsibility

tiva, contravening the principle of culpability; and it is that the existence of fraud or

negligence does not depend on the result, but on the subjective circumstances that

give rise to the alleged infringement.

Regarding the statement that “a third party has gained access to the data

personal data of the holders of the lines”, XFERA considers that it is not “remains

responsible” or “in charge” of any of the treatments to which it gains access.

mislead the offender through received SMS: it is a mere

“third party”, in accordance with article 4 of the RGPD; and third parties are not subject to the

sanctioning system provided for in the Regulation itself or in the LOPD. The res-

responsible for said treatments and, therefore, the subjects obliged to guarantee

czar their security, are exclusively financial entities.

~

Degree of responsibility: the Agency estimates that it is “high”, but, in the opinion of

XFERA, does not justify why, despite the fact that article 83.2.d) RGPD establishes

that should be put in relation to “the technical or organizational measures that

have been applied by virtue of articles 25 and 32” of the same norm. XFE-

RA alleges that it has been proven that there were security procedures

reasonable, in relation to the foreseeable risk for the company at the time

of the facts; and that subsequently, security procedures have been

extraordinarily reinforced, with outstanding results.

~

Categories of personal data affected: XFERA is surprised that the

Agency considers a SIM card to be a category of personal data

whose unauthorized access is “particularly serious”. And who justifies it by saying-

do that "it is not about the personal data that is required for the issuance of the

duplicate of the card, but of the card itself as personal data”. Without em-

However, XFERA considers that SIM cards are not personal data.

nal: they are mere supports, and when a duplicate is activated, they are empty of con-

Dyed. And that there is no category of personal data affected by this

operational, as far as mobile phone operators are concerned, so

This aggravating circumstance does not apply.

SIXTH. On the disproportionate amount of the proposed sanction.

XFERA alleges that, if a total lack of guilt is not found, in any

In any case, a qualified decrease in XFE's culpability should be appreciated.

RA or, at least, of the illegality of the facts of which the pre-

this procedure, which would determine the appropriateness of reducing the severity of the

infractions attributed to it and, therefore, to reduce the sanction to be imposed.

Indeed, considering the previous arguments of guilt, even if they were not

XFERA understands that it could not be ignored that, due to the surrounding circumstances,

current, the behavior displayed is less serious than that considered by the

Agreement. Bearing in mind, furthermore, that practically all the circumstances

aggravating circumstances included therein do not apply to the case, XFERA concludes that only

sanctions that may eventually be imposed should be reduced. Especially when he is-

effort made by XFERA to adapt its security procedures to the new

reality derived from “SIM swapping” is more than remarkable, and its results are exceptional.

nals.

Despite the fact that the amount of the penalty has been significantly reduced with respect to the provided for in the Start Agreement, XFERA considers its amount to be surprising, considering Bear in mind that there have only been 37 cases of SIM swapping; and this because in an infinitely more serious case, in his opinion, which is the one included in the file PS/00179/2020, where a "hacker compromised a series of systems" of the company, having confirmed “that the attacker had collected 488,847 credit cards unique” and had accessed “1,500,000 records”, the fine imposed was €500,000. Y this, despite the fact that the sanctioned company invoiced almost twice as much as XFERA, and that XFERA cooperated to a great extent with the supervisory authority and adopted measures initiatives to alleviate the damage suffered by those affected, as recognized by the Agency.

XFERA understands that the disproportion between one case and another is evident.

For all of the above, XFERA requests that:

a. The completion of the procedure is resolved, with filing of the proceedings, because the Proven Facts do not constitute, in his opinion, in a manifest way party, administrative infraction and the absence of guilt on the part of XFE-

AR; Y

b. Subsidiarily, and only if it is understood that the imposition of a sanction:

Yo. A penalty of warning is imposed exclusively; either

ii. Subsidiarily, that the conduct be classified as an infraction of the

established in article 32 of the RGPD, typified in article 83.4.a) of the ci-

ted Regulation, imposing a maximum penalty of €100,000.

These Allegations will be answered in the FD of this Resolution.

Of the actions carried out in this procedure and the documentation

in the file, the following have been accredited

PROVEN FACTS

FIRST: XFERA is responsible for the data processing referred to in 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, as reported by its

Privacy Policy: “The person responsible will be the company XFERA MÓVILES, S.A.U, with

NIF: A-82528548 and registered office located at Avenida de Bruxelles, 38, 28108, Alco-

bendas (Madrid), Spain. This company offers telecommunications services through

You see different brands such as MÁSMÓVIL, Yoigo, LlamaYa and HappyMóvil.”

SECOND: XFERA provides its mobile telephony services through four brands

commercials analyzed here, which are: YOIGO, MÁSMÓVIL, LLAMAYA and LEBARA.

Each of them has different operating procedures.

THIRD: On October 8, 2019, this Agency received a claim

mation made by the CLAIMANT ONE (file with reference number)

cia E/11270/2019), directed against XFERA, after being issued on September 25

of 2019, a duplicate of the SIM card of the ***TELEFONO.1 line, in favor of a

third person other than the owner of the line -the CLAIMANT ONE-.

These facts were denounced before the General Directorate of the National Police in the

dependencies of Granada Center, on September 26, 2019, with number of

attestation XXXX/XX, in which the CLAIMANT ONE stated the following:

“(…) That the person appearing yesterday around 6:30 p.m. realized

that your mobile phone from the Yoigo company and with terminal number

***TELEFONO.1 was out of service, so it was put into

contact Customer Service of said company, which informed him that

possibly it would have had a problem with the SIM card.

--That today he has appeared at his Bankia bank to

make some payments, indicating the employee that in the current account of his

daughter, named B.B.B. with the same address and contact telephone number as the

appearing was with only 5.60 euros.

--That since the complainant was sure that in said account

there was more money, that is why Bankia employees have verified

what unknown person/s have accessed the phone's online banking

mobile phone of the appearing party and they have withdrawn 1300 euros from the card of the

complainant have transferred it to his checking account at the Bankia entity and to

Then they have made a refund of 1000 euros for the

procedure Charge.Pag friends to the person of C.C.C. and a refund of 150

euros from an ATM, for which you cannot provide data.

--That they have tried to make another withdrawal at the ATM although it has been blocked

the operation.

--That the complainant is an authorized person in his daughter's checking account

B.B.B., so through their mobile phone they have accessed the account of

his daughter and have made three immediate transfers for an amount of 2000

euros, 800 euros and 100 euros, the recipient being DDD.

--That all this information has been indicated by the Bankia employee, since both the complainant and his daughter at no time have had knowledge of what happened and even fewer have authorized the operations indicated. (…)"

In the second of the complaints with report number YYYY/YY, dated 26 September 2019, states:

"(…) On the twenty-sixth day of today, the decedent filed a complaint in these dependencies with number XXXX/XX, in which he gave an account of the extraction fraudulently in his bank account and in the bank account of his daughter, (B.B.B.), for the total amount of 4,050 euros, an event that occurred on the date and right place.

--Appearing again to communicate, that after taking steps with Yoigo's telephone company, it has been reported that the alleged authors of the narrated events made a duplicate SIM card, with the telephone number of the complainant, at the Yoigo office, located in Castellón de la Plana, avenue of the Virgen del Lidón, number 19, with number of duplicity: (ICC) ***NUMBER.1.

--The appearing party wishing to state that he understands that the company Yoigo has provided your personal data, in this case to the person denounced, as well as, has facilitated a duplication of his telephone card, reason why he is completely convinced that he has also been the victim of a criminal offense by said telephone company, by providing your data freely personal. (…)"

It also provides bank receipts in which the following transactions appear made:

- Immediate transfer from the account ***ACCOUNT.3, dated 25

September 2019 at 7:24 p.m., for an amount of 2,000.00 euros in favor of

DDD

- Immediate transfer from the account ***ACCOUNT.3, dated 25

September 2019 at 7:32 p.m., for an amount of 800.00 euros in favor of

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

56/102

DDD

- Immediate transfer from the account ***ACCOUNT.3, dated 25

September 2019 at 9:29 p.m., for an amount of 100.00 euros in favor of

DDD

- Transfer from the account ****ACCOUNT.4, dated September 25,

2019 at 7:07 p.m., for an amount of 1,000.00 euros in favor of C.C.C.

- Reimbursement at an ATM from the account ****ACCOUNT.4, dated 25

September 2019 at 7:19 p.m., for an amount of 150.00 euros.

In relation to this claim, XFERA stated in its response dated July 3

2020, at the request of this Agency, that its fraud department saw signs

that the documentation presented (complaint and DNI attached) together with the application for

SIM card duplicate dated September 25, 2019 was counterfeit.

In its brief of allegations dated March 8, 2021, XFERA affirms that the

criminals managed to deceive the staff of a Yoigo brand store through

the delivery of false documentation, and specifically, a DNI and a report of theft

manipulated by computer programs for image processing.

FOURTH: On November 5, 2019, this Agency received a re-

claim made by the CLAIMANT TWO (file with reference no.

reference E/11591/2019), directed against XFERA, after being issued on July 10,

2019, a duplicate of the SIM card of the line ***TELEFONO.3, in favor of a third

ra person other than the owner of the line -the TWO CLAIMANT-.

These facts were denounced before the General Directorate of the National Police in the

offices of Móstoles, on July 11, 2019, with certificate number

RRRRR/RR, in which CLAIMANT TWO stated the following:

“That the complainant states that he has observed in his account number

***ACCOUNT.1 of the ING entity two charges that he has not made or authorized.

That the movements have been made with the card with the number ***TARJETA.1

which is associated with the account referred to above, being the movements

following:

On 07/10/2019, withdrawal at the ATM number ***CAJERO.1, for a value of

1700 euros.

On 07/10/2019, withdrawal at the ATM number ***CAJERO.1, for a value of

2000 euros.

That he has also appeared at the bank in order to collect the

bank receipt, which contributes to this instruction and is attached to the

presents.

That the deponent states that he has never lost his bank card, stating that

have never made purchases in this establishment.”

In the second of the complaints with the report number SSSSS/SS, dated 29

July 2019, states:

“That these are extensions of the attested number RRRRR/RR of these

dependencies.

That the respondent states that he received a call on 07/26/2019 throughout '

this day without specifying the exact time. (…)

That the call was supposedly made by the caporal number ***NUMBER.2 of the

Mossos d'Esquadra, responsible for theft and fraud.(...)

That said interlocutor asked the complainant to confirm ownership

of the telephone number of which he was a subscriber since it appeared after a series of

investigations that he was carrying out on bank card fraud, that the

His appeared on a list of defaulters. (…)

That his interlocutor then asked him to forward the complaint that

filed, in order to include her in the investigations that were being carried out

by his police unit (...)

That in said telephone conversation that police agent assured him that his

mobile phone through the stores of the "MASMOVIL" company would have been the

place from which at some given moment the duplication of its

card, a fact that in this regard the complainant would remember that days prior to the

materialization of the fraudulent charges on your account and for what you filed with

after denouncing, he realized that for a short time his phone

phone was left without a line and unusable, therefore having to change its SIM card.

(…)"

It also provides bank receipts in which the following transactions appear

made:

- Enable position for the choice of security key for the E.E.E. client,

with NIF ***NIF.2, dated July 11, 2019 at 10:08:37 a.m., at the Office of

Mostoles of the ING Bank.

- Reimbursement at an ATM from the account ***ACCOUNT.1, dated 10

July 2019, for an amount of 1,700 euros.

- Reimbursement at an ATM from the account ***ACCOUNT.1, dated 10

July 2019, for an amount of 2,000 euros.

In relation to this claim, XFERA stated in its response dated March 9

October 2020, at the request of this Agency, that the channel through which it was activated

this SIM was the phone number and provides the appropriate recording as Document No. 19.

Listening to the recording, it is verified that the operator asks for the line number and the

operator himself tells him the name and asks if it is him. It does not ask for the ID number

either.

In its brief of allegations dated March 8, 2021, XFERA affirms that all

indicates that the impersonator got hold of a “blank” SIM card, probably after

Obtain it illegally from a store or from a Masmóvil installation technician. Thus

follows from the content of the call, in which it is verified that the applicant

had the full ICCID of the SIM card, which is only printed on the

back of the card itself.

FIFTH: for the Yoigo brand, in its response dated January 30, 2020, XFERA

indicates that your SIM duplication request procedure was as follows:

- Face-to-face channel: (...)

- Remote channel: (...)

In document No. 6 that accompanies your response brief dated January 30,

2020, XFERA attaches the YOIGO procedure to request a duplicate Card-

ta SIM, which contains the following:

(…)

In document No. 4 that accompanies your response brief dated January 30,

2020, XFERA attaches the cases in which the security policy of all

companies of the MASMOVIL Group for the duplication of SIM Cards, in which

It is known that this must be passed, among other assumptions, (...).

In document No. 1 that accompanies your response brief dated July 3,

2020, XFERA attaches the YOIGO security policy, in which it is stated that (...),

among others. In this document, it is stated that this policy consists of requesting from the holder

of the line: (…)".

In document No. 2 that accompanies your response brief dated July 3,

2020, XFERA attaches the instructions to request a duplicate SIM card, in

which is indicated that (...). And what to ask for a duplicate Sim (...).

SIXTH: for the MásMóvil brand, in its response dated January 30, 2020,

XFERA indicates that its SIM duplication request procedure was as follows:

- Face-to-face channel (...).

- Non-face-to-face channel: (...) In the event that the request originated from theft

of the terminal or SIM card, (...).

In document No. 5 that accompanies your response brief dated January 30,

2020, XFERA attaches the MásMóvil procedure to request a duplicate Tar-

SIM card, which contains the following: "First of all, remember that you will have to pay

set security policy". And the steps to follow are described below: (…).

In document No. 4 that accompanies your response brief dated January 30,

2020, XFERA attaches the cases in which the security policy of all

companies of the MASMOVIL Group for the duplication of SIM Cards, in which

It is known that this must be passed, among other assumptions, (...).

In document No. 5 that accompanies your response brief dated January 30,

2020, XFERA attaches the procedure for SIM duplication of the MasMóvil brand, in

which indicates that (...).

In document No. 6 that accompanies your response brief dated July 3,

2020, XFERA attaches the MásMóvil procedure for requesting duplicates of

SIM cards. This document indicates that since June 22, 2020, the

goes the (...). And that “to request the duplicate we must pass the Security Policy”.

In document No. 7 that accompanies your response brief dated July 3,

2020, XFERA attaches a copy of the MásMóvil security policy. In this document

This document indicates that “The security policy is the questions that we will ask the holder

or user of a line to do any management:

(…)

Among the cases in which a security policy must be passed, it is mentioned (...).

In document No. 8 that accompanies your response brief dated July 3, 2020,

XFERA attaches the ICC activation procedure for MásMóvil (in tests in

that moment). This document indicates (...). And it appears as a security policy

dad:

(…)

SEVENTH: for the Llamaya brand, in its response dated January 30, 2020,

XFERA indicates that its SIM duplication request procedure was as follows:

- Face-to-face channel (...)

- Remote channel: (...)

In document No. 4 that accompanies your response brief dated January 30,

2020, XFERA attaches the cases in which the security policy of all

companies of the MASMOVIL Group for the duplication of SIM Cards, in which

it appears that (...).

In its letter dated July 3, 2020, XFERA stated that "(...)".

In document No. 4 that accompanies your response brief dated July 3, 2020,

XFERA attaches the security policy for the Llamaya brand. In this document,

indicates that

(…)

Among the cases in which a security policy must be passed, “(…)” is mentioned.

In document No. 5 that accompanies your response brief dated July 3, 2020,

XFERA attaches the activation procedure and request for SIM card duplicates

of Llamaya, in which it is stated that (...).

EIGHTH: for the Lebara brand, in its response dated January 30, 2020, XFE-

RA indicates that his SIM duplicate request procedure was as follows:

- Face-to-face channel: (...)

- Remote channel: (...)

As with the rest of the brands, (...).

In document No. 4 that accompanies your response brief dated January 30,

2020, XFERA attaches the cases in which the security policy of all

companies of the MASMOVIL Group for the duplication of SIM Cards, in which

It is known that this must be passed, among other assumptions, (...).

In document No. 3 that accompanies your response brief dated July 3, 2020,

XFERA attaches the SIM card duplication request procedure for the

Lebara brand- remote channel. This document indicates (...).

Regarding the security policy, the document in question indicates that (...) when

you already have the card.

You must pass the security policy at two levels.

(…)

NINTH: In document No. 3 that accompanies your response brief dated 30

January 2020, XFERA attached a screenshot of an internal communication

MÁSMOVIL from Customer Service in which it is indicated "Recently they are de-

Detecting incorrect practices by agents when identifying clients

and apply the security policy. A reminder has been published in ***HERRAMIENTA.1

tory of the process and have sent to all agencies to make them aware of the

importance of the topic. (…)".

Also attached are screenshots from Customer Service (...) in which

indicates "Yesterday we published information of absolute relevance in ***TOOL-

TA.1 about the process that agents must follow to make a correct identification

cation of customers. Following this process is crucial to detecting fraud and ensuring

proper use of private data (such as usernames and passwords

for access to their private areas), being strictly prohibited from requesting

data directly to the client. (…)".

TENTH: Regarding the sending of the SIM card by mail, in your reply to

date January 30, at the request of this Agency, XFERA stated that, with ca-

general character, at the time of requesting a duplicate SIM Card and that it be

Proceed to send it through a messaging system through the Service

Customer Service, the customer must accept the security policy.

The delivery of the duplicate SIM card is carried out through the service “***SERVI-

CIO.1”, (…). Attached as document 2 of this writing are two examples of delivery notes

of delivery in which it is reflected that "The undersigned declares that the shipment reviewed

has been duly: Delivered” and below is the name and surname of a person

(which coincides with the recipient of the shipment) and a DNI/PASSPORT/NIE, together with a

signature.

(…)

In its response brief of July 3, 2020, at the request of this Agency,

XFERA stated that the casuistry by which a client can request the sending of a

duplication of the SIM to a different address is varied: (...).

In document number 9 that accompanies this document, a copy of the co-operation contract is attached.

commercial agreement between XFERA and ***COMPANY.1, dated October 5, 2018,

whose purpose is to designate *** COMPANY.1 as "collaborator for the delivery, on behalf of

bre and on behalf of Masmovil, of SIM cards without activating Masmovil customers”.

In the seventh clause of this contract it is indicated that "In the event that in order to

be able to provide MASMOVIL with the Services, *** COMPANY.1 must process data of character

ter personnel whose person in charge is MÁSMOVIL, ***EMPRESA.1 will act in the name and

on behalf of the latter, assuming the consideration of the person in charge of the treatment, all

this in compliance with article 28 of the RGPD and other applicable regulations.

as well as in accordance with the provisions of the Treatment Order Contract.

attached to this Agreement, as Annex 1, as an inseparable part

of the same".

The documentation provided does not provide any details about the service that

pays *** COMPANY.1 regarding the proper identification of the holders of the lines

object of duplicate SIM for the delivery of the cards in question.

ELEVENTH: Regarding whether the performance of the controls for the verification of the

identity of the applicant for the duplicate SIM card is reflected, for each application

attended, in the Information System of the entity, in its response letter

dated January 30, 2020, at the request of this Agency, XFERA stated

that the most relevant actions during the year 2019 to ensure the rights

of customers have been for each brand:

~

Yoigo: in July 2019, custody began in addition to a physical copy of the con-

SIM duplicate deal, digital copy of the contract plus a copy of the DNI in your

document manager.

~

Masmovil/Llamaya: since the beginning of 2019, a contra-

change of SIM, together with said contract it is established as necessary the

Collection of a copy of the DNI or identity document.

~

Pepephone: in July 2019, documentation begins to be generated and safeguarded

that proves the change of SIM.

Attached as Document 3 is an example of a recording of the request for a duplicate of

MASMOVIL SIM. In this recording, the agent requests the phone number of the line.

line in question and to confirm that it is the owner, full name and

DNI. Next it asks if you went to ***COMPANY.1 to look for the new SIM card

or to a store. And asks for the last four numbers "of a super long number"

that appears on the card under the barcode. The data does not match in a pri-

first time, but the agent finally finds the card associated with that number and,

to confirm the data, you tell the full number of the ICC code to the person who

phone.

TWELFTH: Regarding the reasons why it has been possible in some cases

sos the impersonation of the identity of clients for the issuance of duplicate SIMs,

in its response brief dated January 30, 2020, at the request of this

Agency, XFERA has stated that:

~

~

for the face-to-face channel: it has been possible to produce it by presenting documents

falsified identification (DNI and/or complaint for loss or theft of documentation and

phone) and by human error; Y

for the telephone channel: it could have been caused by human error of the teleoperator.

delivery service personnel, due to the use of falsified documentation.

gives in the delivery and for knowledge of all the personal data of the client.

THIRTEENTH: Regarding the actions undertaken when one of the

these cases, in its response brief dated January 30, 2020, at the request of

of this Agency, XFERA has stated that the following procedure is followed

which has been distributed among the Customer Service teams:

~

"From risk, when they locate a fraud, they will inform the client that they have

to go to a dealer for a new SIM card. They will leave the line with

a blockade and they will also open a ticket in ***APLICACION.1 of impersonation of

identity so you can follow up.

~

You will have to make filters throughout the day (they should not enter

more than 2-3 cases a day) and try to get in touch with the owner, to confirm

sign that you have purchased the new SIM card (…)

(…)

~

FOURTEENTH: Regarding the actions undertaken to prevent cases of

this type are produced again, in his letter dated January 30, 2020, upon request.

development of this Agency, XFERA has stated that in September 2019 it began

to design new rules in the fraudulent traffic monitoring tool

for the detection of possible fraudulent duplicates, these rules analyze

(...).

During the month of November 2019, the tool was configured and validated.

giving the operation in addition to carrying out active surveillance during office hours.

On November 28, 2019, the service was opened (…). Attached as document 10
the corresponding procedure manual. In the "Change SIM MasMóvil" section,
indicates that (…). In the event of not identifying consistency in the use of the line,
will have to contact the client to indicate that for security reasons it is necessary to
confirm if you have made a SIM change (...) in the last few hours. If the analysis of
events or customer contact confirm successful SIM change becomes
to activate the reception of SMS in Mysim and the possible fraud ticket is closed.
A series of identifying features are highlighted that may help to identify those
The cases where there is a possible fraudulent SIM change:

~

(…)

In the “Change SIM Yoigo” section, it is indicated that when a possi- bility alert is activated,
ble fraud (...).
“the client will be contacted to indicate that for security reasons
You need to confirm if you have made a SIM change in the store in the last few hours.
flush”.
If the analysis of the events is correct and there are no indications of fraud, the
analysis performed and the alert is closed.
If indications of possible fraud are identified, ***APPLICATION.1 is opened with the case identified.
tified.
It is highlighted that there are a series of identifying features that can help to identify
Identify those cases where there is a possible fraudulent change of SIM and detail the
same assumptions listed in the Yoigo section, outlined above.
Regarding the management of the SIM duplication confirmation call, it is detailed

the following script:

(…)

In its brief of allegations dated March 8, 2021, XFERA states that it does not

was aware of the criminal operation known as "SIM swapping" until

receives a request from the Telecom User Service General Subdirectorate.

ammunition, from the Secretary of State for Digital Advancement (SEAD), dated 25

September 2019, which is provided as Document 2 and which begins:

“In this Subdirectorate General queries and complaints have been received about

a fraud with the following operation: certain personal data is previously obtained

Personal information of a user (such as the DNI, or checking account number). Starting from those

data, whoever intends to commit the fraud requests the operator, with the data

personal previously obtained, a duplicate of the SIM card. From there, one

Once achieved, financial transactions can be made by accessing the services

Internet financial services, since these include as a security mechanism,

obtaining a key that is sent to the mobile phone (which would be accessed

by duplicating the SIM card).

Also in its brief of allegations dated March 3, 2021, XFERA provided

provided more details regarding the automatic fraud detection system that has been implemented

planted, which consists of a computer tool called “***HERRAMIEN-

TA.2” and that it is a filtering system that is applied (…). In case one

request is detected as potentially fraudulent, the system triggers an alarm,

so that a technician can check if the case is indeed fraudulent and

apply the relevant protocol. The system is activated based on factors such as the following:

following:

(…)

It is also explained that a random review of those applications has been implemented.

card duplication not detected as suspicious by the system “***TOOL-

LIE.2”. This review is carried out at night by the department of

service control, and takes into account factors such as:

(…)

The main action, in case of suspicion, is the immediate blockade in sending and receiving

tion of SMS messages; in addition to trying to contact the owner of the line to see

Verify that you have indeed requested a duplicate of your SIM card.

Regarding the effectiveness of the measures, the 2020 statistics are provided:

Concept

SIM card duplicates made

Potentially fraudulent activation attempts detected

Quantity

***QTY-

DAD.1

***QTY-

DAD.2

Percentage

***PERCENT-

TAGE.1

***PERCENT-

TAGE.2

DAD.5

DAD.4

DAD.3

TAGE.5

TAJE.4

TAGE.3

***QTY-

***QTY-

***QTY-

***PERCENT-

***PERCENT-

***PERCENT-

Fraudulent attempts that exceeded the security policy

(1st layer)

Fraudulent attempts that passed ***TOOL.2

(2nd layer)

Fraudulent attempts that passed random review (3rd

layer)

XFERA states that the implementation of these measures added cumulative effectiveness

***PERCENTAGE.9 side; and represented an effective reduction of ***PERCENTAGE.10

in cases where criminals achieved their illicit goals. is provided,

as Document 6, a table with the ***NUMBER.3 cases that passed the first

barrier.

FIFTEENTH: Regarding the number of cases of fraudulent requests for duplication

SIM crashes detected throughout the year 2019, in its response dated March 30,

January 2020, at the request of this Agency, XFERA stated that they detected

*** AMOUNT. 7 cases in total, (...).

In its pleadings brief dated March 8, 2021, XFERA stated that (...)

cases detected annually in 2019 were intrusion tests carried out by the person

of the company's security, with fictitious data, in order to evaluate the robustness of

existing procedures. Therefore, this figure must be reduced by (...)

fewer cases.

It is also indicated in this pleadings brief that in 2020 the number of cases is re-

led to ***QUANTITY.5.

SIXTEENTH: As for the total number of mobile telephony customers, in its re-

setting date January 30, 2020, at the request of this Agency, XFERA manifests

It stated that it had 4,739,191 postpaid clients and 1,758,708 prepaid clients.

SEVENTEENTH: In its letter dated July 3, 2020, at the request of this

Agency, XFERA provides a list with "the first 20 cases of request for duplicate

fraudulently confirmed SIM cards" since January 1, 2020. From this list,

only two of the cases have been claimed or denounced directly by the client.

The rest of the cases started as a result of an alert generated by the tool.

XFERA ta to detect, among other things, requests for duplicate SIM cards

fraudulent by detecting patterns (tool described in the fact pro-

bad fourteenth). The table provided was as follows:

DATE

05/01/2020

01/14/2020

01/15/2020

01/20/2020

01/25/2020

01/27/2020

01/27/2020

01/28/2020

02/04/2020

02/25/2020

02/27/2020

02/29/2020

03/03/2020

05/03/2020

05/03/2020

03/11/2020

03/13/2020

04/03/2020

04/04/2020

04/08/2020

04/12/2020

MSISDN

***PHONE.4

***PHONE.5

***PHONE.6

***PHONE.7

***PHONE.8

***PHONE.9

***PHONE.10

***PHONE.11

***PHONE.12

***PHONE.13

***PHONE.14

***PHONE.15

***PHONE.15

***PHONE.16

***PHONE.12

***PHONE.17

***PHONE.18

***PHONE.19

***PHONE.20

***PHONE.21

***PHONE.22

BRAND

MoreMobile

Yoigo

MoreMobile

MoreMobile

Yoigo

MoreMobile

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

MoreMobile

MoreMobile

Yoigo

Yoigo

CHANNEL

Telephone

Store

Telephone

Telephone

Telephone

Telephone

Store

Store

Telephone

Telephone

Telephone

Telephone

Telephone

Telephone

Telephone

Store

Telephone

Telephone

Telephone

Store

Telephone

In its letter dated October 9, 2020, at the request of this Agency, XFERA

provides as Documents 1 to 8 duplicates and copies of the DNI provided in the applications

des made in the store of the list in question. It is made clear that in relation to the

***TELEFONO.21 it has not been possible to locate the documentation because it is re-

linked to a possible credential theft. In this case, the store where you buy

that the duplicate has been requested states that it has not been processed in their store.

gives. This impersonation was carried out during the state of alarm, which makes it difficult to investigate

tigation and there is no certainty about the store's claim.

From the documentation provided, it is verified that:

~

In three of the cases, a copy of the applicant's DNI and identification document are provided.

SIM change.

~

In one case they provide a copy of an identity document from the Italian Republic-

na. The SIM change document states that a NIF has been provided and

as DNI/NIF number the number of the Italian identification document, which

which is not correct.

~

It is observed that in two of the cases the DNI have some of the same data,

changing the names (same CAN (Card Identity Number), date of issue)

tion, names of parents and the same handwritten signature).

In this same writing, XFERA provides, for cases of telephone request, such as Do-

documents nº 9 to 18 copy of the recordings of the conversations where the applicant-

The SIM card exceeds the security policy and copies of the recordings of the conversions.

situations where the SIM activation requester exceeds the security policy.

It is clarified that it has not been possible to locate some of the calls, possibly due to

errors in their coding (nomenclature), which makes it difficult to locate them.

tion, given that when calls to service control or customer service are made

zan from the baseline are automatically saved to systems, but

when they are made from a different numbering, as in the cases of activation of

duplicates, agents must enter the nomenclature manually, which is sus-

susceptible to coding errors.

From the listening of the ten calls provided, all referring to the activation of the

card, already in the possession of the applicant, who usually mentions that he has received it by message.

jería, the following is verified:

- Case 1: (...). The operator asks for line number. The applicant asks

also by bank account number, mentions that it begins with four de-

finished digits and the operator answers affirmatively.

~

Case 2: (...), asks for line number. The operator mentions that the card

It is usually sent activated.

- Case 3: The operator asks (...).

- Case 4: The operator asks (...).

- Case 5: The operator asks (...).

- Case 6: The applicant says (...).

~

Case 7: Question line number. At no time does he ask for ID or name.

The operator calls the applicant by their first name. The operator tells you the

New card PIN without asking the applicant.

- Case 8: Question (...).

- Case 9: Question (...). The applicant asks for the invoice amount of 51.33

euros and postal address to which it was sent. The operator tells you the address

invoice delivery.

- Case 10: Question (...).

In its brief of allegations dated March 8, 2021, XFERA indicates that one of

The cases on this list, the one related to the line ***TELEFONO.5, is being investigated.

do by way of penalty by the Court of Instruction no. 9 of Alicante, within the framework of the

preliminary proceedings ÑÑÑÑÑ/ÑÑÑÑÑ. It is attached, as Document 1, official letter of the aforementioned

court dated January 23, 2021, addressed to XFERA, in which it is requested that

provide “the IMEI number of the mobile terminals where the card has been used

SIM associated with the number ****PHONE.5”.

In its brief of allegations dated March 8, 2021, XFERA provides as Do-

Documents 7, 8, 9, 10 the recordings of the five calls that had not been located.

previously due to an error in the encoding (this is when the call is

performed from a different line than the one on which the query is concerned, and the operator

rador does not record this circumstance manually in the customer service systems.

company customer).

Document 7 provides a recording corresponding to the line ***TELEFONO.4

dated January 5, 2020 for the activation of the new SIM card. In which

applicant provides (…), but only remembers the last three digits of the

line number. The agent gives you the full number of the phone line. And the

applicant tells you the number that appears on the new SIM card.

Document 8 provides a recording corresponding to the line ***TELEFONO.7

dated January 20, 2020 for the activation of the new SIM card. In which

Applicant provides his (…). The applicant also indicates the ICC number of the card.

SIM card.

Document 9 provides a recording corresponding to the line ***TELEFONO.10

dated January 27, 2020 for the activation of the new SIM card. In which

Applicant provides his (…). The operator doubts because the sending of the duplicate of the

card does not appear in the system and check with a colleague. She tells him to ask her

the ICC of the old SIM card. The operator asks for the ICC of the old SIM card,

but the applicant says that he lost the previous card. And the operator tells him that he must

go to a store. The applicant states that he cannot go to a store. The opera-

The dora consults her coordinator and he tells her that she can activate the card if she has passed

do the security policy and have the ICC number of the new card.

Document 10 provides a recording corresponding to the line ***TELEFONO.13

dated February 25, 2020 for the activation of the new SIM card. In which

applicant provides (…). The operator hesitates because sending the duplicate of the tar-

jeta does not appear in the system. It is she who gives him the complete number of the line.

After being asked, the applicant also provides the ICC code of the card that is

allegedly received from ***EMPRESA.1, which does not match what appears in the system.

ma. After making some queries, the operator asks you to confirm the surnames of the

holder, which the applicant correctly provides. And it asks again for the ICC code,

after which the activation of the SIM is processed.

Document 11 provides a recording corresponding to the line ***TELEFONO.19

dated April 3, 2020 for the activation of the new SIM card. in which the so-

bidder provides (…).

In its pleadings brief dated March 8, 2021, XFERA reproduces a table

bla where the twenty claims contributed at the time to the

Agency, but incorporating the date and time the illicit request was received and the

SIM card lock. Note that three of the numbers are repeated

two because the fraudulent operation was intercepted twice by the system

of security.

MSISDN

***PHONE.4

***PHONE.5

BRAND

MoreMó-

vile

Yoigo

CHANNEL

Telephone

Store

Request

05/01/2020

22:12

01/14/2020

Blocking

05/01/2020

22:24

01/15/2020

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

***PHONE.6

***PHONE.7

***PHONE.8

***PHONE.9

***PHONE.10

***PHONE.10

***PHONE.11

***PHONE.12

***PHONE.13

***PHONE.14

***PHONE.15

***PHONE.15

***PHONE.16

***PHONE.12

***PHONE.17

***PHONE.18

***PHONE.19

***PHONE.20

***PHONE.21

MoreMo-

vile

MoreMó-

vile

Yoigo

MoreMó-

vile

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

Yoigo

MoreMó-

vile

MoreMó-

vile

Yoigo

Telephone

Telephone

Telephone

Telephone

Store

Store

Store

Telephone

Telephone

Telephone

Telephone

Telephone

Telephone

Telephone

Store

Telephone

Telephone

Telephone

Store

***PHONE.22

Yoigo

Telephone

20:18

01/15/2020

12:43

01/20/2020

21:01

01/25/2020

16:48

01/27/2020

14:20

01/27/2020

17:07

01/27/2020

19:56

01/28/2020

12:29

02/04/2020

16:08

02/25/2020

23:05

02/27/2020

18:31

02/29/2020

21:38

03/03/2020 7:37

05/03/2020

17:07

05/03/2020

21:07

03/11/2020

13:59

03/13/2020

12:51

04/03/2020

15:11

04/04/2020

13:45

04/08/2020

21:03

04/12/2020

15:39

21:43

01/15/2020

13:20

01/20/2020

22:51

01/25/2020

17:50

01/27/2020

17:50

01/27/2020

17:28

01/27/2020

21:50

01/28/2020

12:59

02/04/2020

16:26

02/25/2020

23:12

02/27/2020

19:19

02/29/2020

21:51

03/03/2020 7:48

05/03/2020

22:23

05/03/2020

21:37

03/11/2020

14:42

03/13/2020

13:24

04/03/2020

15:22

04/04/2020

14:04

04/08/2020

22:04

04/12/2020

15:54

In 10 of the 22 listed above, the ***TOOL.2 system detected the

possible fraud and XFERA staff managed to contact the owner of the line, blockade

keeping the duplicate card before the criminals achieved their goal, until

where it is known: ***PHONE.4, ***PHONE.8, ***PHONE.10 (on two occasions

nes), ***PHONE.11, ***PHONE.14, ***PHONE.18, ***PHONE.19,

***PHONE.21, ***PHONE.22. The mean blocking time, in the cases listed

two, it was 40 minutes; and its median, 31 minutes.

In a total of 9 out of the 22 listed above, the ***TOOL.2 system

detected the possible fraud and, despite the fact that XFERA staff did not get contact

to have with the owner of the line, the possibility of receiving SMS on the duplicate card was blocked.

each before the criminals achieved their goal, as far as is known: ***TE-

PHONE.6, ***PHONE.10, ***PHONE.12 (on two occasions), ***PHONE-

PHONE.13,

***PHONE.17,

***PHONE.20. The average block time, in the listed cases, was 43 minutes.

utes; and its median, 19 minutes.

C/ Jorge Juan, 6

28001 – Madrid

(on two occasions),

***PHONE.15

www.aepd.es

sedeagpd.gob.es

68/102

In the case of the number ***TELEPHONE.16, the system of ***TOOL.2 does not de-

detected the possible fraud, but the XFERA service control audit did (ter-

wax security layer), blocking the duplicate card. It turned out to be a “false positive”

vo”: the client contacted the company days later, to request its unblocking.

In two cases, the ***TOOL.2 system did not detect the fraud, and it was the pro-

own clients who contacted XFERA, after detecting that their line was not working

correctly: ***PHONE.5, ***PHONE.7.

Of these two cases, it is important to point out that, regarding the telephone number

***PHONE.5, identity theft occurred in (...), and that the applicant

exhibited a false DNI, a copy of which was provided to the file.

EIGHTEENTH: Regarding the possibility of obtaining a SIM without associating it with

a telephone line, in his letter dated October 9, 2020, at the request of

this Agency, XFERA stated that it only knows of two cases:

1. Submission of replacement cards, which are not activated and are not associated with any line.

To prevent fraud from occurring in the activation of these SIMs, the

Procedure of (…).

2. Lots of SIMs from (…). These SIMS are not intended to replace a SIM of a

active client, but provide them to clients who have requested a portability

at the time of installation.

XFERA's fraud department has detected that the SIMs whose activation is

has requested by telephone and they have turned out to be impersonations, (...). It is unknown

ce the circumstances in which the "usurpers" get hold of these SIMs.

NINETEENTH: As to whether SIM duplication cases have been detected

fraudulent in which there is previously a change of ownership supplanting

keeping the identity of the old owner, so that, later, the new owner performs the

change of SIM, in its letter dated October 9, 2020, XFERA stated that it did not

No cases have been reported so far. As document No. 20 is attached the pos-

security policy that is passed to the applicant in changes of ownership by telephone

AC. This document indicates that:

“The security policy is the questions that we will ask the owner or user of a policy.

line to do any management:

(…)

It is also indicated that the security policy must be passed, among other cases, in a

"Change of ownership".

This document also states that for the change of owner for mobile only and con-

vergence, "The client must send by mail to Cambiotitular@masmovil.com, the following

documentation:

(…)

Indicates that (…).

As document No. 21, the procedure for the change of ownership is attached. In this

document indicates that “To change the owner of a line, the current owner and the new

They don't have to go to a store together (Yoigo or The Phone House depending on where they are).

discharged) and present the following documentation (...)”. This document in-

It also includes the security policy in which it is indicated that it must be requested (...).

TWENTIETH: As to whether information was provided to the workers about the

verification of the security elements of the DNI and passport, in your letter of

response to the Resolution Proposal of this sanctioning procedure, XFE-

RA provides as Document 1 a presentation with the brand "Yoigo", dated July
2013, which is entitled "Procedure for the Identification of Falsified Documentation-
gives", in which information is given on the tools used for the detection of
documentation (…)".

FOUNDATIONS OF LAW

FIRST: Competition.

By virtue of the powers that article 58.2 of the RGPD recognizes to each Authority of
Control, and according to what is established in articles 47, 48, 64.2 and 68.1 of the LOPDGDD, the
Director of the AEPD is competent to initiate and resolve this procedure.

In initiating the sanctioning procedure, the AEPD has acted in accordance with the
general principles of article 3.1 of the LRJSP, among which is the service
citizens, good faith, legitimate expectations or transparency of the
administrative action.

The AEPD has attributed a series of competencies, powers and functions provided for in
Articles 55 and following of the RGPD that according to article 8 of the LRJSP,
They are inalienable and will be exercised by the administrative bodies that have them attributed.
taken as their own.

In the exercise of the functions and powers attributed to it by articles 57 and 58 of the
RGPD, controls the application of the RGPD, conducts investigations and imposes, where appropriate,
administrative sanctions which may include administrative fines, and
orders the corresponding corrective measures, according to the circumstances of each
particular case. Thus, you can carry out the investigations you deem appropriate (ar-
Article 67 of the LOPDGDD), after which you can decide to initiate an ex officio procedure
sanctioning party (article 68 LOPDGDD).

In the case examined, the investigations carried out in order to determine the co-
mission of some events and their scope revealed the existence of

insufficient security measures, which caused improper access to data

personal information, which has directly affected the duty to maintain the 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

XFERA, 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 XFERA despite having some

security measures that should be adopted in the processing of personal data

necessary for the provision of the contracted services and throughout their cycle

of life, these measures have been clearly insufficient to prevent access

due to fraudulently requested SIM card duplicates.

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. Taking into account the nature, scope, context and purposes of the treatment

as well as risks of varying probability and severity to the rights and freedoms

of natural persons, the data controller will apply technical measures

and appropriate organizations in order to guarantee and be able to demonstrate that the treatment is

in accordance with this Regulation. These measures will be reviewed and updated

when needed.

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.
On the other hand, in accordance with the principle of proactive responsibility that the RGPD conse-
gra in its article 5.2, the AEPD cannot indicate any data controller
what are the security measures to be implemented, since only the latter is aware
in depth of your organization, of the treatments that it carries out, of the risks
associated with them and the precise security measures to be implemented to
enforce the principle of integrity and confidentiality.
However, it has been proven that the measures implemented by XFERA are 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 focus on the deficient configuration of the questions formulated in the security policy in order to obtain the duplicate SIM card.

Thus, from the documentation sent by XFERA it is verified that different checks to prove the identity of the person making the request or activation of the duplicate of the SIM card according to the brand in question.

In general, the personal data associated with the security policy are the basic ones of any client: (...). In some cases (LLAMAYA) the request of the (...), basic data also associated with any client. It is enough to have basic data physical data of a client in order to overcome the security policy, without any pre-additional question is formulated with respect to some data known only to the operator and his client. No supplementary requirement is required.

It is striking that only some of the brands carry out additional checks. more rigorous information, such as usage data that only the person using the line in question could answer correctly. Thus, with respect to the LEBA-RA establishes the overcoming of the security policy in two layers, appearing in second of them the formulation and correct answer of two or three questions of use to verify very specific data that could reliably identify the client.

This shows that XFERA did have very simple security measures in place. most appropriate to reliably identify a customer and did not implement in all its brands.

In addition to the security measures implemented after the commission of the proven facts and that are valued positively by this Agency, the truth is that the offense has been committed. For all the above, we focus the facts on the information

Fraction derived from article 5.1.f) of the RGPD.

Thus, the fraud known as "SIM Swapping" is a criminal technique

consisting of obtaining a duplicate of the SIM card associated with a telephone line

ownership of a user, in order to impersonate their identity to obtain access

so to your social networks, instant messaging applications, banking applications,

rias or electronic commerce, in order to interact and carry out operations in your

name, authenticating by means of a username and password previously taken from

that user, as well as with the double factor authentication when receiving the confirmation SMS.

mation in their own mobile terminal where they will have inserted the duplicate SIM card.

It should be noted that in the first phase of this type of scam the impersonator considers

fraudulently mislead login details or online banking credentials

of the client, but he needs to be able to know the verification code, second factor of increase

authentication, to be able to execute any operation. The moment you achieve

the duplicate SIM card already also has access to this second authentication factor.

tion and, therefore, from that moment you can carry out the acts of patrimonial disposition

nial you want.

Returning to the analysis of the security policy used by XFERA for the verification

proof of the identity of the person requesting or activating the duplicate SIM card, and

As an example, presumably criminals who have already obtained a series

data such as access data or online banking credentials of a person

person and the phone line number associated with that account, you probably already have

so with the basic information of that person, such as their name and surnames and

number of personal identification. This Agency cannot consider that sufficient

mere verification that is clearly useless for the purposes for which it is

planned.

In summary, it is the responsibility of the operator to establish adequate requirements

effective and efficient that, although a quick reading may seem very strict,

a much more careful reading has shown that they were not. Whereupon, the

scam or impersonation, which apparently could seem complex and difficult, it is seen that

it has not been so due to the inadequacy of the security measures at the time of

ensure that it is the owner of the SIM card or the person authorized by him who requests

the duplicate, which denotes a lack of due diligence in risk management in

question.

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;

XFERA 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 (hereinafter, Law 25/2007),
requires that holders of all SIM cards, whether prepaid or contract, be
be duly identified and registered. This is important because the identification
cation of the subscriber will be essential to register the SIM card, which entails
It will be necessary that when obtaining a duplicate of this, the person requesting it must
also identify themselves and that their identity coincides with that of the holder.
In short, both the personal data (name, surnames and DNI) that are processed to issue
Get a duplicate SIM card as your own SIM (Subscriber Identity Module) card
that uniquely and unequivocally identifies the subscriber in the network, are character data
personal data, and its treatment must be subject to data protection regulations.
cough.
FIFTH: Allegations adduced to the Resolution Proposal.
We proceed to respond to them according to the order set out by XFERA:
FIRST. Disagreement with the qualification of the alleged infraction.
Article 5 “Principles related to treatment” provides: “1. The personal data is
will: (...) f) treated in such a way as to guarantee adequate security of the data

personal 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 ("integrity and confidentiality").

In this case, the principle of data confidentiality has been compromised.

given that access was facilitated to some duplicates of SIM cards requested in a

fraudulent. And this access occurred because XFERA did not have measures

sufficiently appropriate in the terms of the aforementioned article 5.1.f) of the RGPD in order to

to prevent these events from occurring. In this regard, reference is made to what is stated in the

FD Third of this Resolution.

For its part, it should be noted that the 2021 Report of the State Attorney General's Office

dedicated to "Computer Crime" dedicates in its point 8 a mention to the current

Fraudulent online promotions:

“In this brief review of online fraudulent actions, it is necessary to

mention of the behaviors that affect the telecommunications sector

in its different variants, and closely related to them, although the damage

generated in online banking, commonly known as SIM fraud

Swapping, which is being used with alarming frequency in recent

years. The technique consists of circumventing the security measures of the entities

banking des accessing the alphanumeric codes of confirmation, of

single use, generated on the occasion of electronic transactions and that

They are ordinarily communicated to clients through SMS messages.

To do this, criminals previously obtain a duplicate or a new
a SIM card in the name of his victim, either by requesting it from the operator co-
responding, simulating the identity of that, either using a
more elaborate methodology, as in the supposed object of judicial instruction
in Zamora, in which an establishment was used for this purpose.
mobile repair service. Once they have the SIM card at their disposal
tion, criminals are guaranteed to receive on their own device the
confirmation code of the fraudulent transaction and, ultimately, the possibility
ability to make it effective for their benefit, avoiding that at that time
moment is known by the injured party. This form of defraud
in recent years has generated multiple police investigations
and the initiation of legal proceedings in different territories such as A
Coruna and Valencia. Its effectiveness and the ease with which criminals
achieve their illicit purposes has determined the adoption by operators
telephony of specific measures of prevention and strengthening of the
guarantees for the issuance of these cards or their duplicates."
The disputed facts are considered of sufficient relevance and seriousness, as
to subsume them in a violation of article 5.1.f) of the RGPD, precisely, because
that the security of customer data has not been guaranteed -adequately-
da-, and consequently, there has been an unauthorized and illegal treatment that
affects the confidentiality of data and that has resulted in other consequences, nothing
trivial, such as economic damage, that would not have occurred if XFE-
RA, would have ensured the correct identity and authentication of its clients.
The security measures must guarantee that in our organization the data of
personal character are only used for the legitimate purpose for which they were collected, unless
ble legal exceptions. Periodic checks must be carried out to verify

They want and value the effectiveness of the security measures that we have implemented.

And of course there is an application cost, which requires time, which in turn

Sometimes they must be in accordance with the regulations and the state of the art, but it is that, to be

select the appropriate security measures, the person in charge must base himself on the

risks for natural persons, as well as what is reasonable and technically possible.

possible. Article 28.2.a) of the LOPDGDD establishes some cases in which it is already

It is clear that it is necessary to contemplate greater risks than those that the person in charge could

estimate if he only took into account his own interests (identity usurpation, damage to

economic prices…).

For all these reasons, the allegation made by XFERA regarding the inadequate interpretation

principle of specialty declines, since the Proven Facts are included in the

They perfectly comply with the violated article 5.1.f) of the RGPD. This precept, which is not

vague or abstract, establishes clear compliance obligations - prevent treatment

unauthorized or illegal by implementing appropriate security measures - whose in-

fraction determines a typical behavior, for whose commission the operator is now sanctioned.

radora.

Furthermore, we must mean that XFERA confuses the typification of the

infringements provided for in the RGPD, sections 4 and 5 of article 83 of the RGPD, with the typi-

fication for the mere effects of the prescription foreseen in articles 72, 73 and 74 of

the LOPDGDD, for the purposes of your right of defense. Thus, the operator considers

that the LOPDGDD typifies another behavior that fits much more exactly to the

course of fact, which is the one provided for in article 73.f) of the LOPDGDD.

Well, the LOPDGDD's own statement of reasons clarifies that "The categorization

The infractions are entered for the sole purpose of determining the deadlines for

prescription, having the description of typical behaviors as the only object

enumeration in an exemplary manner of some of the punishable acts that

should be understood as included within the general types established in the European standard.

pee".

The typical behavior is framed, as it has been motivated, in the article

5.1.f) of the RGPD constituting an infringement typified in article 83.5.a) of the

GDPR; As a consequence of the foregoing, it is typified directly and immediately as

a very serious infraction for the mere effects of the prescription in article 72.1.a)

of the LOPDGDD. This is the way that the RGPD marks to typify infractions

and not another.

Likewise, it cites PS/00362/2021 and PS/00179/2020 in its defense, having to

point out that it is perfectly admissible that the AEPD has considered the violation

of a certain precept in the conviction that it is more in line with the facts

that occur, without this action being qualified as arbitrary, especially when

is duly motivated.

In relation to PS/00362/2021, note that XFERA collects as if they were Facts

Proven what is contained in the claim presented in the sanctioning procedure

to which we now refer, that is, "The grounds on which the claim is based are that

the claimed one facilitates the detail of the last movements of the Affinity Card

through an automated telephone service system on the phone ******** in the

that only the client's DNI is requested as identification data. manifested by

the complainant that the entity complained against does not adopt any other security measures

to confirm the identity of the client so that anyone can call, give

a DNI number and obtain information associated with that DNI, without verifying that the

caller is the holder of said identification document". The truth is that the

claim is formulated because a client detects insufficient security measures

reason for which they are sanctioned, without the client denouncing the transfer of their data to

a third party (the verbal tense in which the content of the claim is collected may

imply otherwise, but no such possibility was concluded from the proceedings

previous investigation), nor that it be accredited at any time in the procedure

sanctioning party that data had been transferred to third parties.

As for PS/00179/2020, it comes from the notification of a security breach,

generated by the intervention of a hacker who directly steals personal data from

clients of the database of the company that suffers the security breach, which

does not in itself constitute a transfer of data by the data controller.

I lie to a third party. Conducted the appropriate investigations and verified what happened

do, they were sanctioned for lack of security measures.

From the examination of the concurrent facts in the present case and the actions

of investigation carried out, as well as the instruction of the sanctioning procedure

It has been considered for this assumption now examined that there has been a vulnerability

neration of article 5.1.f) of the RGPD, considering that the actions of the Agency

were intended to analyze the procedures applied to change requests

of SIM card. The SIM card constitutes the physical support through which access to

the personal data of the affected person. If its availability is not guaranteed

tion and control, access to the personal data of the owner, as well as the possible use or uses

by third parties, it becomes a threat that can have devastating effects

in the lives of these people.

It must be remembered that the right to data protection derives from the EC, which establishes

establishes the limitation of the use of informatics by the Law to guarantee the honor and intimacy

personal and family life of citizens and the full exercise of their rights

(article 18.4).

The Constitutional Court indicated in its Judgment 94/1998, of May 4, that we

We are faced with a fundamental right to data protection that guarantees

gives the person control over their data, any personal data, and over their

use and destination, to avoid illicit traffic of the same or harmful to the dignity and

rights of those affected; in this way, the right to data protection is confi-

figure as a faculty of the citizen to oppose that certain personal data

nals are used for purposes other than the one that justified their obtaining.

For its part, in Judgment 292/2000, of November 30, it considers it as a

autonomous and independent right consisting of a power of disposition and control

on 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 can

collect, and that also allows the individual to know who owns that personal data

and for what, being able to oppose that possession or use.

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.

In the investigation of the procedure it has been verified that a

adequate security in the processing of personal data, taking into account the

result that produced identity theft. That is, a third party gained access

access to the personal data of the holders of the lines without the security measures

of XFERA, they could avoid it.

Therefore, XFERA has not demonstrated compliance with

the principles relating to the processing of affected personal data.

SECOND. XFERA has not broken the principle of data confidentiality.

The SIM card identifies a phone number and this number, in turn, identifies your

headline. In this sense, the Judgment of the CJEU in case C -101/2001 (Lindqvist) of

6.11.2003, section 24, Rec. 2003 p. I-12971: “The concept of "personal data" that

uses Article 3(1) of Directive 95/46 includes, in accordance with the

definition that appears in article 2, letter a), of said Directive "all information on

an identified or identifiable natural person". This concept includes, without a doubt, the

name of a person together with their telephone number or other information regarding

their working conditions or their hobbies”.

Also, this opinion is singled out in relation to mobile telephony devices

that allow the location of the interested party, in Opinion 13/2011 on services

of geolocation in smart mobile devices (document WP185):

“Smart mobile devices. Smart mobile devices are inextricably

ably linked to natural persons. Normally there is a different identifiability

straight and indirect First, the telecommunications operators that provide

They provide access to the mobile Internet and through the GSM network they normally have a

registration with the name, address and bank details of each client, along with va-

various unique numbers of the device, such as the IMEI and IMSI. (…)"

Likewise, the Judgment of the Court of Justice of the European Union (CJEU) of 19

October 2016 Case C-582/14, considers that even the dynamic IP address has

to be considered personal data to the extent that the service provider

cios has means can know the identity of the holder of that IP address of a character

dynamic.

Or the most recent STJUE of June 17, 2021 Case C-579/19 that in its section

102 recalls that "(…) A dynamic IP address registered by a service provider

online media services on the occasion of the consultation by a person of an In-

internet that that provider makes accessible to the public constitutes with respect to said pro-

sees personal data within the meaning of article 4, point 1, of the Regulation

2016/679, when he has legal means that allow him to identify the person.

interested person thanks to the additional information available to the provider of ac-

Internet access of that person (...).

This means that as long as there is the possibility of carrying out the identification, we will be

We are dealing with personal data.

This consideration is important in relation to the specific case, as remember

that the dynamic IP address is one that changes from time to time, for example

by changes in the network, or by the reboot of the device with which the service provider services the connection provides, as opposed to the static IP address that it is always the same.

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 and the IMEI (International Mobile Station Equipment Identity), which have a permanent character and from which it derives, therefore, a better individualization of the user and also his identification, can also have have such consideration.

Therefore, it follows that both the IMEI and the IMSI to the extent that they allow sin- to regularize an individual, and therefore to identify him, must be considered data of character. personal nature in accordance with article 4.1 of the RGPD that considers as such: Any information about an identified or identifiable natural person ("the data subject"); I know An identifiable natural person shall be considered any person whose identity can be determined be identified, directly or indirectly, in particular by means of an identifier, such as example a name, an identification number, location data, an identifier online or one or more elements of the physical, physiological, genetic, psychological, economic, cultural or social of said person.

Likewise, the Judgment of the Provincial Court of Barcelona no. 390/2019 of 30 May, provides: "However, the identity of the holder of the SIM card, or what is same, the identity of the holder of the telephone number associated with said card, not constitutes traffic data derived from telephone communications or data affect the communication itself. There is no doubt that it constitutes a personal datum. nal relative to the intimacy of the person protected in art. 18.1 EC.”

THIRD. Violation of the principles of personality of the sanction and typi- city.

The processing operations that are the subject of this file are related to

with the exercise of the rights that as end users of community services

electronic cations are being made by the operator's customers. In this sense, the

regulations in this sector confer a public nature both to the provision itself

of the service (“services of general interest”) as well as to the specific regime of protection

of users (“obligations of a public nature”).

Within the specific rights of this sector, the regulatory regulation is

found in the Bill of Rights of the user of electronic communications services

case (Royal Decree 899/2009, of May 22). In its article 5 (Celebration of contra-

cough) the following is specified:

"two. Operators may not access an end user's line without their consent.

express and unequivocal statement.

It should be remembered that the facts prosecuted in this file have consisted

precisely in that, that is, in the improper issuance of SIM cards that

have allowed third parties outside the line to access it. It is therefore affected

the right of the end user that is considered a public obligation

co.

But not only that, but in attracting customers, and particularly in ex-

requesting SIM cards, it is necessary to comply with the provisions of Law 25/2007. This law

It is dictated in use of state competence in matters of public security, and has

in order to guarantee that the operators conserve and make available to the Forces

and Security Bodies, the data relating to the holders of community services

electronic calls and their traffic data. Article 2 establishes the following:

“They are recipients of the obligations related to the conservation of data imposed

in this Law the operators that provide electronic communications services dis-

available to the public or exploit public communications networks, in the established terms.

established in Law 32/2003, of November 3, General Telecommunications.”

Article 3 and, specifically for prepaid lines, the single additional provision,

establishes that all end users holding services must be identified

of electronic communications.

As has been proven in this file, the points of sale and centers of

answering telephone calls were used for the issuance of duplicates of

SIM cards. For these purposes, it would be applicable, in the identification of clients, the

mentioned Law 25/2007.

Therefore, they are involved in the management of clients by the operators.

telecommunications carriers, aspects directly related to services

of general interest, obligations of a public nature and, above all, public security.

public of the State.

However, these aspects cannot be addressed by the operators of

in any way, violating the data protection regulations in whatever is applicable.

cable. Although a specific character is recognized, it is no less true that none of them

In some way they can be considered a waiver for the protection of a fundamental right.

fundamental as is the right to the protection of personal data of individuals

duos. And it is the obligation of telecommunications operators, such as XFERA, to provide

the aforementioned service by implementing appropriate security measures, which guarantee

They comply with the principle of confidentiality of the personal data of the

that the operator in question is responsible.

For its part, regarding the liability of financial institutions, the Directive

PSD2, applies to payment services provided within the Union (Article 2), and does not

to XFERA, but it is also true that issuing a duplicate SIM card to

favor of a third party who is not the owner of the line, provides impersonators with the

control of the telephone line, and therefore of the SMS addressed to the linked telephone

to the initial SIM card and in this way to be able to access to know the authentication code.

transaction certification.

Pursuant to article 4.30 of the Directive, “strong authentication” is based on the use

lization of two or more elements categorized as knowledge (something that only co-

knows the user), possession (something that only the user owns), and inherence (something that is

the user). These elements or factors are independent of each other and, therefore, the vulnerability

generation of one does not compromise the reliability of the others.

The basis is very simple: the more elements you have to verify the

identity of the user, the more secure the transaction.

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 that you wish to carry out, the impersonator will receive, normally through

of an SMS, an alphanumeric verification code on the mobile phone linked to that

profile. Said code has a limited temporary validity and is for a single use, that is,

it is only generated for that particular transaction and for a limited time.

Once the verification code was entered, the transaction would be carried out and completed.

tion. It is assumed that only the user has the mobile device in his possession (it would be the

"something you have"), so when you receive the verification code on said mobile phone

Through SMS, your identity would be doubly authenticated. Therefore, to the

planters would not be enough to be able to commit fraud with knowing the user and

password with which the victim identifies, but it will be necessary to intercept

have said confirmation code. Consequently, in order to carry out a transfer

non-consensual non-consensual purchase, transaction or purchase, that is, to carry out the fraud

automatically, the cybercriminal must illegitimately access the verification codes

associated with each of these operations sent by the bank through

of SMS and the most common way to do it is by obtaining a duplicate

SIM card drop.

Therefore, it is necessary to execute two completely different but compatible actions.

complementary to each other.

First of all, you have to obtain the access data to the online banking or provider

of payment owned by the person to be defrauded, if we focus on the search for the

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.

Well, in the last of these actions -obtaining the duplicate-, it is where

focused on the facts that are the object of this procedure and not on those that occurred in the first

ra phase, which are outside the responsibility imputed to XFERA.

As for the responsibility of the criminals who carry out these frauds, there is no doubt

Possibly, it is outside the responsibility imputed to XFERA in the present

penalty procedure.

Regarding the SIM card provided when a duplicate of this is provided

is empty and personal data processed by XFERA is not accessed, we refer to

section 2 of this FD.

In relation to the fact that XFERA is the mere intermediary of the messages that are sent and

receive through these fraudulently obtained SIM card duplicates, from

in accordance with the provisions of article 14.1 of the LSSI and that in any case it would be

in the event of a violation of the secrecy of communications, which is not the responsibility of

the AEPD, we reiterate that it is not the object of this sanctioning procedure what

occurs in the phase prior to obtaining the duplicate SIM card (obtaining the

data necessary to carry out the fraud) nor what happens in the phase after obtaining

the mentioned duplicate of the SIM card (the illicit enrichment through the access

so to the bank account of the affected and the use of the codes that are sent through

see that SIM card). The purpose of this sanctioning procedure and what

responsibility is attributed to XFERA is solely for providing a person

other than the holder access to a duplicate of his SIM card for not having implanted

appropriate security measures to prevent such fraud.

QUARTER. Violation of the principle of culpability.

4.1. XFERA had not identified the risk, simply because it did not exist before

PSD2.

The violation of the imputed administrative infraction responds to a precept included

within “Principles related to treatment” that requires confidentiality to be ensured.

security of personal data through adequate security in the treatment of

personal data, security that has not been guaranteed in accordance with the Facts

Tested.

In this procedure, the risk existing before the

application of the PSD2 call but the one produced from your application, which is

when the type of fraud detailed in the previous sections begins to be carried out

by using a duplicate SIM card improperly obtained by per-

It sounds different from its owner.

Thus, the infraction occurred not because of the lack of security measures for the ex-

request for SIM duplicates, but because of the need for their revision and reinforcement.

It is not enough to have security measures, but they must be adapted

to mitigate risks. The continuous advancement of technology and the evolution of treatments

These practices favor the continuous appearance of new risks that must be managed.

In this context, the GDPR requires data controllers to implement

adequate control measures to demonstrate that the rights and freedoms are guaranteed

individuals and data security, taking into account, among others, the

“risks of varying probability and severity to the rights and freedoms of individuals

physical persons” (article 24.1) applying the appropriate measures.

In the present case, the security measures implemented are not sufficient.

to guarantee the confidentiality of the personal data in question, as has been

explained in detail in section 1 of this FD.

4.2. XFERA acted in the belief that the person requesting the duplicate was

who he claimed to be.

The condition of victim of XFERA is not discussed, but the unauthorized access to a du-

SIM card problem, which is considered particularly serious as it makes it possible to replace

plantation of identity with a purpose, that of interacting and carrying out operations in

name of a third party.

XFERA cannot deny the fact that it processes personal data on a large scale.

the. It is the operator itself that acknowledges having more than 4 million postpaid customers.

go and more than one and a half million prepaid customers.

Indeed, in sanction matters the principle of culpability governs (STC 15/1999,

from July 4; 76/1990, of April 26; and 246/1991, of December 19), which means

that there must be some kind of fraud or fault. As the STS of January 23,

1998, "...we can speak of a decided jurisprudential line that rejects in the ambit

sanctioning mechanism of the Administration strict liability, requiring the con-

recurrence of intent or negligence, in line with the interpretation of the STC 76/1990, of 26

April, pointing out that the principle of culpability can be inferred from the principles of law

legality and prohibition of excess (article 25 of the Constitution) or the demands

inherent in the rule of law".

Lack of diligence in implementing security measures at source

adequate to verify that the person requesting or activating the duplicate of a

SIM card is the holder of this is precisely what constitutes the element of the

culpability.

As for XFERA being the victim of fraud, it should also be noted that XFERA

must be in a position to establish mechanisms that prevent the occurrence of

fraudulent duplication of SIM cards, measures that respect the integrity and confi-

confidentiality of the data and that prevent a third party from accessing data that is not of

its ownership, since it is precisely the operator's responsibility to process data of a personal nature.

according to the RGPD (recitals 76, 77, 78, 79, 81 and 83 RGPD; article 32 of the

RGPD and article 28 of the LOPDGDD)

Periodic testing, measurement and evaluation of the effectiveness of the measures

technical and organizational measures to guarantee the security of the treatment are the responsibility

of each person responsible and in charge of the treatment in accordance with article 32.1.d) of the

GDPR.

Therefore, XFERA as data controller is obliged to verify both

selection as the level of effectiveness of the technical means used. The exhaustion

vity of this verification must be evaluated through the prism of adequacy to the risks

costs and proportionality in relation to the state of technical knowledge, the costs

implementation details and the nature, scope, context, and purposes of the treatment.

treatment.

As the instructor indicated in the proposed resolution, in the cases described

in the section of Proven Facts, the security of the data of the

effectively, and in particular, its correct custody to avoid loss, theft

or unauthorized access.

Certainly, the principle of responsibility set forth in article 28 of the LRJSP, dis-

states that: “They may only be sanctioned for facts constituting an admissible infraction.

natural and legal persons, as well as, when a Law recognizes them as

capacity to act, affected groups, unions and entities without personality

legal entity and independent or autonomous estates, which are responsible for

the same by way of fraud or guilt.”

However, the mode of attribution of liability to legal persons is not

corresponds to the forms of willful or reckless guilt that are attributable

to human behavior. So, in the case of offenses committed by persons

legal rules, although the element of guilt must concur, it applies

necessarily differently from how it is done with respect to natural persons.

According to STC 246/1991 "(...) this different construction of the imputability of the auto-

ria of the infraction to the legal person arises from the very nature of legal fiction

to which these subjects respond. They lack the volitional element in the strict sense.

but not the ability to break the rules to which they are subject.

Capacity for infringement and, therefore, direct blame that derives from the legal right

co-protected by the rule that is violated and the need for such protection to be

really effective and for the risk that, consequently, must be assumed by the legal entity

which is subject to compliance with said rule" (in this sense STS of 24 November

November 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

also be tested, must be considered in order to assume the correspondence

tooth load, which ordinarily the necessary volitional and cognitive elements

to appreciate it are part of the typical behavior tested, and that their exclusion

requires that the absence of such elements be proven, or in its normative aspect,

that the diligence that was required by the person who alleges its non-existence has been used; No

suffices, in short, to exculpate a typically unlawful behavior.

with the invocation of the absence of guilt".

The ultimate responsibility for the treatment continues to be attributed to the controller

of the treatment, who is the one who determines the existence of the treatment and its purpose. Re-

Let us agree that, in general, the operators treat the data of their clients by

protection of the provisions of article 6.1 b) of the RGPD, as it is considered a treatment

necessary for the execution of a contract in which the interested party is a party (...). By

Therefore, it is the responsibility of the operators (XFERA, in the present case) to implement

take appropriate measures to ensure compliance with the principle of confidentiality

ciality enshrined in article 5.1.f) of the RGPD, so that, if such principle is seen

compromised due to a lack of diligence in implementing sufficient measures

cient for it, the responsibility of such infraction will be imputed to the operator in

question.

FIFTH. Circumstances applicable to the individual case, in accordance with art. 83.2

GDPR.

We refer to the Seventh FD.

SIXTH. On the disproportionate amount of the proposed sanction.

Regarding the breach of the principle of proportionality, the RGPD expressly provides

mind the possibility of graduation, through the provision of fines likely to

modulation, in attention to a series of circumstances of each effective individual case.

ve, proportionate and dissuasive (article 83.1 and 2 RGPD), general conditions

for the imposition of administrative fines that have been analyzed by

this Agency, to which must be added the graduation criteria provided for in the LO-

PDGDD, object of development in the Seventh FD.

It should be noted that the agreed administrative fine will be effective because it will lead

the company to apply the technical and organizational measures that guarantee a degree

security corresponding to the criticality value of the treatment.

It is also proportional to the violation identified, in particular its seriousness, the

circle of natural persons affected and the risks that have been incurred and to the following

financial position of the company.

And finally, it is dissuasive. A dissuasive fine is one that has a dissuasive effect.

sory genuine. In this regard, the Judgment of the CJEU, of June 13, 2013, Ver-

salis Spa v Commission, C-511/11, ECLI:EU:C:2013:386, says:

“94. Regarding, first of all, the reference to the Showa Denko/

Commission, cited above, it should be noted that Versalis interprets it incorrectly.

correctly. In fact, the Court of Justice, when pointing out in paragraph 23

of said judgment that the dissuasive factor is valued taking into consideration

tion a multitude of elements and not only the particular situation of the company.

in question, he was referring to points 53 to 55 of the Preliminary Opinion.

seated in that matter by Advocate General Geelhoed, who had

pointed out, in essence, that the dissuasive multiplier coefficient

may have as its object not only a 'general deterrence', defined as a

action to discourage all companies, in general, from trading

not only the offense in question, but also a 'specific deterrent',

consisting of dissuading the specific defendant from re-infringing

turn the rules in the future. Therefore, the Court of Justice only confirmed,

in that sentence, that the Commission was not obliged to limit its assessment

factors related only to the particular situation of the company.

prey in question."

“102. According to settled jurisprudence, the objective of the multiplier factor

suasory and the consideration, in this context, of the size and resources

global objectives 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,

do, see, in particular, the judgment of June 17, 2010, Lafarge/Co-

mission, C-413/08 P, Rec. p. I-5361, section 104, and the order of February 7

2012, Total and Elf Aquitaine v Commission, C-421/11 P, paragraph 82).”

The Judgment dated May 11, 2006 issued in the cassation appeal

7133/2003 establishes that: “It must also be taken into account that one of the criteria

governing the application of said principle administrative sanctioning regime (criterion

collected under the rubric of «principle of proportionality» in section 2 of article

131 of the aforementioned Law 30/1992) is that the imposition of pecuniary sanctions does not

must suppose that the commission of the typified infractions is more beneficial

for the offender than compliance with the rules violated”.

Also important is the jurisprudence resulting from the Judgment of the Third Chamber

of the Supreme Court, issued on May 27, 2003 (rec. 3725/1999) that

says: Proportionality, pertaining specifically to the scope of the sanction,

constitutes one of the principles that govern the sanctioning Administrative Law, and

represents an instrument of control of the exercise of the sanctioning power by the

Administration within, even, the margins that, in principle, the standard indicates

applicable for such exercise. It certainly supposes a concept that is difficult to determine

a priori, but which tends to adapt the sanction, by establishing its specific graduation
within the indicated possible margins, to the seriousness of the constitutive act of the
infraction, both in its aspect of unlawfulness and culpability, weighing
as a whole the objective and subjective circumstances that make up the budget
de facto punishable -and, in particular, as it results from article 131.3 LRJ and PAC, the
intentionality or repetition, the nature of the damage caused and the recurrence
Inc-. (SSTS July 19, 1996, February 2, 1998 and December 20, 1999, en-
three many others).

In any case, given the allegation made by XFERA regarding the disproportion of the
fine stating that "only" there have been 37 cases of SIM swapping, reiterated
It should be noted once again that the AEPD, as a result of 37 claims for identity fraud, which im-
The person responsible for the treatment requested the issuance of a duplicate of the card.
ta SIM of the customer (after which there have been serious economic damages to the
affected) investigates in depth the origin of the problem in order to find out if or
was due to a flaw in the privacy protection model.

The focus is not on the third parties that have exceeded the security policies, but
in why they have overcome them; that is, the condition, characteristics and
adequacy of the policies cited to the data protection regulations and the current
information from the data controller in this regard.

SIXTH: Principles relating to treatment.

Considering the right to the protection of personal data as the right
natural persons to have their own data, it is necessary to determine the
principles that make it up.

In this sense, article 5 RGPD, referring to the "Principles related to treatment"
has:

"1. The personal data will be:

a) processed in a lawful, loyal and transparent manner in relation to the interested party ("lawful

trust, loyalty and transparency»);

b) collected for specific, explicit and legitimate purposes, and will not be processed further.

riorly in a manner incompatible with said purposes; (...);

c) adequate, pertinent and limited to what is necessary in relation to the purposes for

those that are processed ("data minimization");

d) accurate and, if necessary, updated; All reasonable steps will be taken

entitled to delete or rectify without delay the personal data that

are inaccurate with respect to the purposes for which they are processed (“accuracy”);

e) maintained in a way that allows the identification of the interested parties during

no longer than is necessary for the purposes of processing the personal data;

(…)

f) processed in such a way as to ensure adequate security of the data

including protection against unauthorized or unlawful processing and

against its loss, destruction or accidental damage, through the application of measures

appropriate technical or organizational measures ("integrity and confidentiality").

2. The controller will be responsible for compliance with the provisions

in paragraph 1 and able to demonstrate it ("proactive responsibility").

The principle of data security requires the application of technical or organizational measures.

appropriate organizational measures in the processing of personal data to protect said

data against access, use, modification, dissemination, loss, destruction or accidental damage

dental, unauthorized or illegal. In this sense, security measures are key to

when guaranteeing the fundamental right to data protection. It is not possible the

existence of the fundamental right to data protection if it is not possible to guarantee

the confidentiality, integrity and availability of our data.

In this sense, recital 75 of the RGPD determines: The risks to the rights

rights and freedoms of natural persons, of varying gravity and probability, can

are due to the processing of data that could cause physical damage,

material or immaterial, in particular in cases where the processing may

give rise to problems of discrimination, identity theft or fraud, fi-

financial losses, reputational damage, loss of confidentiality of data subject to secre-

professional creed, unauthorized reversal of pseudonymization, or any other per-

significant economic or social judgement; in the cases in which the interested parties are deprived

two of their rights and freedoms or are prevented from exercising control over their data

personal; in cases in which the personal data processed reveal the origin

ethnic or racial, political opinions, religion or philosophical beliefs, militancy

in trade unions and the processing of genetic data, data related to health or social data.

sexual life, or criminal convictions and infractions or security measures such as

nexus; in cases in which personal aspects are evaluated, in particular the analysis

analysis or prediction of aspects related to performance at work, economic situation,

mica, health, personal preferences or interests, reliability or behavior, situation

tion or movements, in order to create or use personal profiles; in cases where

those that process personal data of vulnerable people, in particular children; or in

cases in which the treatment involves a large amount of personal data and

affects a large number of stakeholders.

Likewise, recital 83 of the RGPD establishes: "In order to maintain the security and

avoid that the treatment violates the provisions of this Regulation, the controller

responsible or the person in charge must evaluate the risks inherent to the treatment and apply mea-

given to mitigate them, such as encryption. These measures must guarantee a level of security

adequate security, including confidentiality, taking into account the state of the tech-

uniqueness and the cost of its application with respect to the risks and the nature of the data

personal to be protected. When assessing the risk in relation to the safety of

the data, the risks that derive from the treatment of the data must be taken into account.

personal data, such as the accidental or unlawful destruction, loss or alteration of data

personal data transmitted, stored or otherwise processed, or the communication

or unauthorized access to said data, which is particularly likely to cause damage

and physical, material or immaterial damages".

We must attend to the unique circumstances of the two claims presented.

through which it can be verified that, from the moment in which the loss

impersonating person replaces the SIM, passes control of the line to the persons

you sound impersonating Consequently, the claimants are affected by 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 transactions

Processing of personal data must be lawful and fair. For individuals, you must

be absolutely clear that they are being collected, used, consulted or processed

otherwise personal data concerning them, as well as the extent to which they di-

All data is or will be processed. The principle of transparency requires that all information

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

in 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 of the RGPD provides: "(...) Natural persons must have control
of your own personal data. (…)"
The facts declared previously proven, are constitutive of a violation
of article 5.1.f) of the RGPD by providing XFERA duplicates of the SIM card to third parties
people who are not the legitimate owners of the mobile lines, after overcoming
by people supplanting the security policies implemented by the operation.
dora, which shows a breach of the duty to protect the information of the
customers.

This unauthorized access to the personal data of those affected is determined

te for subsequent actions carried out by the impersonators, since

that take advantage of the space of time that elapses until the user detects the fac-

llo on the line, he contacts the operator, and she detects the problem, to

carry out fraudulent banking operations -which have been reproduced in both cases

denounced - and that without the duplication of the SIM card it would have become impossible to

realization.

The issuance and delivery of the duplicate to an unauthorized third party implies for those affected

two the loss of control of your personal data. Therefore, the value of that data

personal, integrated in a physical support -SIM card-, is real and unquestionable, reason

for which XFERA has a legal duty to guarantee your security, just as it would

with any other assets.

It is worth mentioning ruling 292/2000, of November 30, of the Constitutional Court

tutional, which configures the right to data protection as an autonomous right

and independent that consists of a power of disposition and control over the data

personal data that empowers the person to decide which of these data to provide

to a third party, be it the State or an individual, or what data this third party may collect, and

which also allows the individual to know who owns that personal data and for what,

being able to oppose that possession or use. Thus, in accordance with the legal foundations

cos 4, 5, 6 and 7 of the judgment of the high court:

"4. Without needing to explain in detail the wide possibilities that information

matic offers both to collect and to communicate personal data or the

undoubted risks that this can entail, given that a person can ignore

rar not only what are the data that concern you that are collected in

a file but also if they have been transferred to another and for what purpose, it is enough to indicate both extremes to understand that the fundamental right to privacy (art. 18.1 CE) does not provide sufficient protection by itself in the face of this new reality derived from technological progress.

However, with the inclusion of the current art. 18.4 CE the constituent put of highlighted that he was aware of the risks that the use of the information could entail. and entrusted to the legislator the guarantee of both certain fundamental rights mental and the full exercise of the rights of the person. That is, in- incorporating a guarantee institute "as a form of response to a new formation a concrete threat to the dignity and rights of the person", but which is also, "in itself, a fundamental right or freedom (STC 254/1993, of July 20, FJ 6). Concern and purpose of the constituent which is evident, on the one hand, if one takes into account that from the draft The constitutional text already included a section similar to the current art. 18.4 EC and that this was later expanded by accepting an amendment to include- ra its final paragraph. And more clearly, on the other hand, because if in the debate in the Senate, some doubts were raised about the need for this section of the precept given the recognition of the rights to privacy and honor in the initial section, however, were dissipated by highlighting that these rights, in view of their content, did not offer sufficient guarantees against the threats that the use of information technology could entail for the protection of private life. So the constituent wanted to guarantee through the

current art. 18.4 EC not only a specific scope of protection but also

more suitable than the one that fundamental rights could offer, by themselves.

such mentioned in section 1 of the precept.

5. (…) Well, in these decisions the Court has already declared that art.

18.4 CE contains, under the terms of STC 254/1993, a guarantee institute

of the rights to privacy and honor and the full enjoyment of the remaining

rights of citizens which, moreover, is in itself "a right or freedom

fundamental right, the right to liberty against potential aggressions against

the 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-

privacy of a person's private life and reputation today have a dimension

positive pressure that exceeds the scope of the fundamental right to intimidation.

ity (art. 18.1 CE), and that translates into a right of control over the data

relating to the person himself. The so-called "computer freedom" is thus the right to

control the use of the same data inserted in a computer program (ha-

beas data) and includes, among other aspects, the citizen's opposition to

that certain personal data are used for purposes other than

the legitimate one that justified its obtaining (SSTC 11/1998, FJ 5, 94/1998, FJ 4).

This fundamental right to data protection, unlike the right to

privacy of art. 18.1 CE, with whom it shares the goal of offering efficient

effective constitutional protection of private personal and family life, attributes to

holder a bundle of powers consisting for the most part of the legal power

dictate of imposing on third parties the performance or omission of certain behaviors

ments whose specific regulation must be established by the Law, the one that conforms to art. 18.4 CE must limit the use of information technology, either by developing the right fundamental right to data protection (art. 81.1 CE), either regulating its exercise cycle (art. 53.1 CE). The peculiarity of this fundamental right to protection tion of data regarding that fundamental right as related as that of intimacy lies, then, in its different function, which therefore entails that also its object and content differ.

6. The function of the fundamental right to privacy of art. 18.1 CE is that of protect against any invasion that may be carried out in that area of the personal and family life that the person wishes to exclude from the knowledge of others and of the interference of third parties against their will (for all STC 144/1999, of July 22, FJ 8). Instead, the fundamental right to data protection seeks to guarantee that person a power of control over about your personal data, about its use and destination, with the purpose of preventing its illicit and harmful traffic for the dignity and rights of the affected. Finally, the right The right to privacy allows certain data of a person to be excluded from knowledge. third party, for this reason, and this Court has said so (SSTC 134/1999, of 15 July, FJ 5; 144/1999, FJ 8; 98/2000, of April 10, FJ 5; 115/2000, of 10 of May, FJ 4), that is, the power to protect your private life from publicity No, darling. The right to data protection guarantees individuals a power of disposal over such data. This guarantee imposes on the public powers public authorities prohibiting them from becoming sources of such information without the

due guarantees; and also the duty to prevent the risks that may derive

avoid improper access or disclosure of such information. But that power

of disposition on the personal data itself nothing is worth if the affected

knows what data is held by third parties, who owns it, and

to what end

Hence the singularity of the right to data protection, since, on the one hand,

Its object is broader than that of the right to privacy, since the right

fundamental to data protection extends its guarantee not only to privacy

in its dimension constitutionally protected by art. 18.1 EC, but to

which this Court has on occasion defined in broader terms as

sphere of the assets of the personality that belong to the sphere of private life.

da, inextricably linked to respect for personal dignity (STC 170/1987,

of October 30, FJ 4), such as the right to honor, expressly cited in the

art. 18.4 CE, and likewise, in a very broad expression of art. 18.4 CE, al

full exercise of personal rights. The fundamental right to

Data protection extends the constitutional guarantee to those data that

are relevant to or have an impact on the exercise of any rights

rights of the person, whether or not they are constitutional rights and whether or not they are relative

honor, ideology, personal and family intimacy to any other cons-

formally protected.

In this way, the object of protection of the fundamental right to protection

of data is not reduced only to the intimate data of the person, but to any

type of personal data, whether intimate or not, whose knowledge or use by third parties

ros may affect their rights, whether fundamental or not, because their purpose

it is not only individual intimacy, for this is the protection that art.

18.1 CE grants, but personal data. Therefore, also

reaches those public personal data, which by the fact of being, of being

accessible to the knowledge of anyone, they do not escape the power of disposition

of the affected party because this is guaranteed by their right to data protection. Tam-

Also for this reason, the fact that the data is of a personal nature does not mean that it only

those related to the private or intimate life of the person have protection, but

that the protected data are all those that identify or allow the

identification of the person, being able to serve for the preparation of their profile

ideological, racial, sexual, economic or of any other nature, or that serve

for any other use that in certain circumstances constitutes a

threat to the individual.

But the fundamental right to data protection also has a se-

second peculiarity that distinguishes it from others, such as the right to privacy

personal and family of art. 18.1 EC. This peculiarity lies in its content,

since unlike the latter, which confers on the person the legal power

to impose on third parties the duty to refrain from any interference in the

privacy of the person and the prohibition of making use of what is thus known

(SSTC 73/1982, of December 2, FJ 5; 110/1984, of November 26, FJ

3; 89/1987, of June 3, FJ 3; 231/1988, of December 2, FJ 3; 197/1991,

of October 17, FJ 3, and in general the SSTC 134/1999, of June 15,

lio, 144/1999, of July 22, and 115/2000, of May 10), the right to pro-

data protection attributes to its holder a bundle of faculties consisting of different

those legal powers whose exercise imposes legal duties on third parties, which
are not contained in the fundamental right to privacy, and that serve the
essential function performed by this fundamental right: to guarantee the person
a power of control over your personal data, which is only possible and effective
vo imposing on third parties the aforementioned duties to do. Namely: the right
I agree that prior consent is required for the collection and use of the
personal data, the right to know and be informed about the destination and use of
that data and the right to access, rectify and cancel said data. In defi-
tive, the power of disposal over personal data (STC 254/1993, FJ 7).
7. From all that has been said, it follows that the content of the fundamental right to
Data protection consists of a power of disposition and control over data.
personal data that empowers the person to decide which of these personal data
provide to a third party, be it the State or an individual, or what this third party can
ro collect, and that also allows the individual to know who owns that data
and for what, being able to oppose that possession or use. These can-
disposition and control over personal data, which constitute part
of the content of the fundamental right to data protection are specified
legally empowered to consent to the collection, obtaining and access to
personal data, their subsequent storage and treatment, as well as their
possible use or uses, by a third party, be it the State or an individual. And that right-
right to consent to the knowledge and treatment, computerized or not, of the data
personal, requires as essential complements, on the one hand, the faculty
the right to know at all times who has these personal data and to what
use is subduing them, and, on the other hand, the power to oppose that possession and
applications.

Finally, they are characteristic elements of the constitutional definition of the right fundamental to the protection of personal data the rights of the affected to consent to the collection and use of your personal data and to know of the same mos. And it is essential to make this content effective the recognition protection of the right to be informed of who owns your personal data and with what purpose, and the right to be able to oppose that possession and use by requiring who corresponds to put an end to the possession and use of the data. Namely, requiring the owner of the file to inform him of what data he has about his personal person, accessing their appropriate records and seats, and what fate they have had- do, which also reaches potential assignees; and, where appropriate, require to rectify or cancel them." (the underlining of all the paragraphs is our)

Therefore, any action that involves depriving the person of those faculties disposition and control over your personal data, constitutes an attack and a vulnerability ration of their fundamental right to data protection.

SEVENTH: General conditions for the imposition of the administrative fine.

Article 83.2 of the RGPD provides that:

"Administrative fines will be imposed, depending on the circumstances of each individual case, in addition to or as a substitute for the measures contemplated in art. Article 58, paragraph 2, letters a) to h) and j). When deciding to impose an administrative fine and its amount in each individual case shall be duly taken into account:

a) the nature, seriousness and duration of the offence, taking into account the

nature, scope or purpose of the processing operation in question

as well as the number of interested parties affected and the level of damages and losses.

who have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor

to alleviate the damages suffered by the interested parties;

d) the degree of responsibility of the data controller or data processor.

taking into account the technical or organizational measures that have been applied

under articles 25 and 32;

e) any previous infringement committed by the person in charge or the person in charge of the treatment-

I lie;

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

gave the infringement and mitigate the possible adverse effects of the infringement;

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

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

particular if the person in charge or the person in charge notified the infringement and, in such case,

what extent;

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

previously against the person in charge or the person in charge in question in re-

relationship with the same matter, compliance with said measures;

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

certificates approved in accordance with article 42, and k) any other factor

aggravating or mitigating circumstance applicable to the circumstances of the case, such as the benefits

financial gains obtained or losses avoided, directly or indirectly, through

through the infringement.

For its part, article 76 “Sanctions and corrective measures” of the LOPDGDD provides

ne:

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

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

two in section 2 of the aforementioned article.

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

may also be taken into account:

a) The continuing nature of the offence.

b) The link between the activity of the offender and the performance of treatment of

personal information.

c) The profits obtained as a result of committing the offence.

d) The possibility that the conduct of the affected party could have induced the

violation.

e) The existence of a merger by absorption process subsequent to the commission of

the infringement, which cannot be attributed to the absorbing entity.

The impact on the rights of minors.

F)

g) Have, when not mandatory, a data protection officer.

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

alternative conflict resolution mechanisms, in those cases in which

those that exist controversies between those and any interested party. (…)”

In accordance with the precepts transcribed for the purpose of setting the amount of the sanction

as responsible for the infringement typified in article 83.5.a) of the RGPD, it proceeds

graduate the fine that corresponds to impose, prior assessment of the allegations adduced

for the purposes of a correct application of the principle of proportionality.

On the one hand, the following aggravating factors have been taken into account:

- Article 83.2.a) RGPD:

The nature, seriousness and duration of the offence, taking into account

the nature, scope or purpose of the processing operation that

concerned, as well as the number of stakeholders affected and the level of

damages that they have suffered:

XFERA claims that the SIM card does not have personal information. No ob-

However, this point was already refuted in the Fifth FD, section 2. Also

alleges, that the loss of control of the data of the interested parties

duce in financial entities and that XFERA is a mere third party.

This point was refuted in the Fifth FD, section 3.

As regards the nature of the infringement, the violation of the principle of

article 5.1.f) RGPD entails a significant risk for the rights of

the affected. The Agency considers that the nature of the infringement

It is very serious since it leads to a loss of disposition and control

about personal data. It has allowed criminals to steal identity.

by hijacking the number of the phone number after obtaining

Have a duplicate of your SIM card. After the entry into force of the Directive

tive PSD2, the mobile phone has come to play a very important role
important in making online payments as it is necessary for the confirmation
transaction information, and converts this device -and by extension
to the SIM card-, a clear objective of cybercriminals.
In relation to the time period with respect to which the events occurred,
although the facts denounced by the complaining parties occur
on certain dates, XFERA declared that there were ***QUANTITY
DAD.6 cases in fiscal year 2019 and ***AMOUNT.5 cases in fiscal year
cio 2020.
Regarding the number of interested parties affected: XFERA stated that
produced ***NUMBER.6 cases in fiscal year 2019 and ***NUMBER.5
cases in fiscal year 2020. Therefore, it would be a total of ***AMOUNT.9
affected.
In relation to the level of damages and losses suffered, XFERA alleges
that the damages caused would be limited only to the cost of the
duplicate SIM request, which was already returned to everyone who re-
also claimed that the damages caused by bank fraud
River are not your responsibility. However, this Agency has already
concluded that the responsibility imputed to XFERA is for doing
having provided a fraudulently requested duplicate SIM card
due to the inadequacy of the measures implemented by XFERA to
avoid it.
The Agency considers that the level of damage caused is high, since
that access to duplicates of said SIM cards has resulted in
Fraudulent banking operations that took place in a short space of
weather. By duplicating SIM cards, the alleged su-

planters have gained control of the subscriber line and consequently

I decree the reception of SMS addressed to the legitimate subscriber to carry out

online operations with banking entities supplanting their personalization

dad. These SMS are sent by banking entities as part of the

two-step verification of operations such as money transfers

rias or Internet payments, and access to these SMS is usually the reason

of fraudulent duplication of SIM cards.

It is true that XFERA is not responsible for the identification policies

tion of clients established by the banking entities nor can it be

attribute responsibility for bank fraud. However, it is also

true, that if XFERA ensured the identification procedure and en-

delivery, the verification system of the entities could not even be activated.

bank data. The scammer after getting the activation of

the new SIM, takes control of the telephone line, thus being able to

then carry out fraudulent banking operations by accessing the

SMS that banks send to their customers. this sequence

of facts revealed in the claims filed ge-

would be a series of serious damages that should have been

taken into account in an impact assessment relating to the protection of

data (considering 89, 90, 91 and article 35 of the RGPD). Definitely,

from the moment a duplicate is delivered to a person other than

the owner of the line or authorized person, the customer loses control of
the line and the risks, damages, multiply. In addition, I have
Many happen with overwhelming immediacy.
In short, the application of the aggravating circumstance of article 83.2.a) of the RGPD is
refers to the seriousness of the Proven Facts, which is manifested
this, among other issues, in the social alarm generated by the realization
tion of these fraudulent practices and the very high probability of
materialization of the risk, without the number of claims being decisive.
presented mations. And this, because what has been analyzed in the
present sanctioning procedure are the security measures implemented
by the data controller (XFERA) as a result of various re-
claims filed with the AEPD.
- Article 83.2.b) RGPD:
 Intentionality or negligence in the infringement:
XFERA alleges that it has not been negligent, but that it was misled by
linquent. That, furthermore, negligence does not depend on the result (it is
That is, whether or not duplicate SIM cards were provided to people who
fraudulently requested). And that XFERA is a third party, given
that does not treat the data that is accessed by obtaining fraudulently
dulent of that duplicate SIM card.
As for XFERA not being negligent, but instead being deceived by
offenders, what is explained in the Fifth FD, section 4 is reiterated.
XFERA would have been diligent in implementing adequate measures
adequate to correctly identify the people requesting and activating
SIM cards go, there would be no improper access to them.
Regarding that negligence does not depend on the result, this Agency

considers that there has been a violation of the principle of confidentiality

as a consequence of negligence in the implementation

Take the appropriate measures referred to in article 5.1.f)

of the RGPD to guarantee that confidentiality, as it has been developed

lled in the Third and Fifth FD, section 4.

Regarding the fact that XFERA is a third party, given that it does not process the data to which

accessed by fraudulently obtaining a duplicate card

SIM, what is developed in the Fifth FD, section 3, is reiterated in the sense

that this sanctioning procedure focuses solely on the

phase after obtaining the necessary data for the request for

the SIM card. Nor does it assess XFERA's responsibility for the

time after obtaining that duplicate SIM card, in the

illicit enrichment takes place. Only the attitude is analyzed

XFERA's negligence regarding the provision of a duplicate

SIM card to a person other than its owner without checking correctly

mind if the person requesting it is indeed who they say they are.

Regarding the unlawfulness of XFERA's conduct, it is considered that

responds to the offending type and the title of guilt. XFERA is considered to

has acted negligently. As a repository of personal data

sonal on a large scale, therefore habituated or specifically dedicated

to the management of the personal data of the clients, it must be

especially diligent and careful in his treatment. That is, from

From the point of view of guilt, we are faced with a defeatable error, since with

the application of the appropriate technical and organizational measures, these

identity theft could have been avoided.

Although the Agency considers that there was no intent on the part of

XFERA, concludes that it was negligent in not ensuring a procedure

that guarantees the protection of the personal data of the clients.

Thus, a socially harmful result is produced that imposes

disapproval of the implemented security policy resulting in

was ineffective, regardless of the level of commitment shown,

which is unquestionable.

Deny the concurrence of negligent action on the part of XFERA

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 involves continuous work

treatment of customer data, indicates that "... the Supreme Court is coming

understanding that there is recklessness whenever a duty is neglected

legal duty of care, that is, when the offender does not behave with the

due diligence. And in assessing the degree of diligence, it must be

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.

It is established as fundamental the risk analysis of the treatment of

data according to the specific circumstances of the operator, such

such as volume and type of data. It is vitally important to establish and

implement the necessary procedures and measures, based on the

characteristics and entity of this, that allow to demonstrate that it has had

I have done due diligence in trying to prevent the occurrence of

an identity theft. Thus, although the damage has been done

made by a third party outside the company, it must be possible to demonstrate that

The necessary precautions have been taken during the development of the

business activity, required by the regulations, to avoid damage

that was predictable. It is about having an objective level of care

depending on the specific circumstances of the case that makes it possible to

Make sure you were aware of the possibility of being impersonated

of identity, and that, with this, the appropriate measures were applied to

reduce the materialization of such a risk to the minimum possible.

- Article 83.2.d) RGPD:

 Degree of responsibility of the data controller or data processor

taking into account the technical or organizational measures that

already applied under Articles 25 and 32:

XFERA alleges that it is not justified why its grade was assessed as "High"

of responsibility, since it had adopted adequate measures

according to the foreseeable risk.

In this regard, this Agency considers that the responsibility of the

rabilities in the procedure for the issuance of the duplicate tar-

SIM card corresponds to XFERA, which is the legal entity to whom the

appropriate measures must be implemented to prevent the occurrence of

lead to situations like the ones analyzed here.

Since it has been concluded that XFERA lacked these adequate measures,

sisters, is considered responsible for not having done everything

could be expected to do, especially when you have the means of

all kinds more than sufficient to adequately comply, given

account of the nature, purposes or scope of the processing operation

in light of the obligations imposed by the RGPD.

- Article 83.2.g) RGPD:

 Categories of personal data affected by the breach:

XFERA alleges that the SIM card is not personal data and that, therefore,

to, there is no category of affected data. However, this ob-

conservation was already analyzed in the Fifth FD, section 2. In conclusion,

this Agency considers that the SIM card is personal data and
which, as such, has a particularly sensitive nature, since it can
enables identity theft.
The delivery of a duplicate SIM in favor of a third party other than the lender
legitimate owner is considered particularly serious since it makes it impossible to
sending or receiving calls, SMS, or access to data service,
which happens to be in the hands of the supplanting person.
Obtained the duplicate, the path to the applications and ser-
vices that have as a key recovery procedure the en-
sending an SMS with a code to be able to change the passwords. In
In addition, it enables identity theft.
And although they have not been affected "Special categories of data
personal" as defined by the RGPD in article 9, this does not mean that
the stolen data was not of a sensitive nature. It's not about the
personal data that is required for the issuance of the duplicate of the tar-
card, if not the card itself as personal data associated with a line
telephone number of a user, which is obtained for the purpose of subscribing
plant your identity to gain access -among others- to applications
banking or electronic commerce, in order to interact and perform
perform operations on your behalf, authenticating through a user and
password previously taken from that user, as well as with the autho-
double factor authentication when receiving the confirmation SMS in your pro-
own mobile terminal where the duplicate SIM card will be inserted.

~

Article 76.2.b) LOPDGDD:

 Linking the activity of the offender with the performance of treatment

personal data:

The development of the business activity carried out by XFERA requires

re continuous and large-scale processing of the personal data of

customers, according to the number of mobile voice lines reported

called by XFERA (4,739,191 postpaid customers and 1,758,708

prepaid customers, in 2019), which positions XFERA as one of the

the four largest telecommunications operators in our

country.

On the other hand, the following mitigating factors are taken into consideration:

- Article 83.2.c) RGPD:

 Measures taken by the person responsible to mitigate the damages

suffered by the interested parties:

positive.

Namely:

(…)

- Article 83.2.f) RGPD:

 Degree of cooperation with the supervisory authority:

Tall.

The Agency considers that XFERA has cooperated favorably with

research, providing answers to most of the requirements

ments and forming part of the working group of this Agency regarding

to the problem of duplicate SIM cards, which is valued

Positive way.

- Article 76.2.c) LOPDGDD:

 The benefits obtained as a result of the commission of the investment

fraction:

This Agency does not consider that XFERA has obtained an economic benefit

beyond receiving the price of the cost set for the issuance of

duplicate SIM cards.

- Article 76.2.h) LOPDGDD:

 Submission to conflict resolution mechanisms:

Various telecommunications operators, including

XFERA, signed a Protocol with AUTOCONTROL that, without prejudice

tion of the powers of the AEPD, provides mechanisms for the

private resolution of controversies related to data protection in

the field of contracting and advertising communications services

electronically, dated September 15, 2017. Protocol whose application

effective cation should be considered as mitigating.

The allegations adduced by XFERA in relation to the article are rejected.

83.2.a), b) and c), as stated in this same FD.

The aggravating factor provided for in article 83.2.e) of the

RGPD, after considering that the aforementioned sanction is not pertinent or relevant in relation to

with the sanctioning procedure now processed (considering 148 of the RGPD).

We have applied the same destination to the mitigating factor provided for in article 76.2.a) of

the LOPDGDD, regarding the continuous nature of the infraction, since the lack of concurrence

rrence of the budget for its application entails that it cannot be taken in con-

consideration, following the criteria expressed by the SAN, Contentious-Administrative Chamber

nistrative, Section 1, of May 5, 2021, Rec. 1437/2020, which says: "Consider, for

On the other hand, that the non-commission of a previous infraction should be considered as a mitigating factor.

river. Well, article 83.2 of the RGPD establishes that it must be taken into account to

the imposition of the administrative fine, among others, the circumstance "e) any infraction

committed by the person in charge or the person in charge of the treatment". This is a

aggravating circumstance, the fact that the budget for its application does not

tion implies that it cannot be taken into consideration, but does not imply or allow,

as claimed by the plaintiff, its application as a mitigating factor".

Therefore, in accordance with the applicable legislation and after assessing the graduation criteria

tion of the sanctions whose existence has been accredited, the director of the AEPD,

RESOLVES:

FIRST: IMPOSE XFERA MÓVILES, S.A., with NIF A82528548, for an infringement

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

as very serious for prescription purposes in article 72.1.a) of the LOPDGDD, a

administrative fine amounting to 200,000'00 (two hundred thousand euros).

SECOND: NOTIFY this resolution to XFERA MÓVILES, S.A.

THIRD: Warn the sanctioned party that she must enforce the sanction imposed

Once this resolution is enforceable, in accordance with the provisions of

article 98.1.b) of the LPACAP, within the voluntary payment term established in article

Article 68 of the General Collection Regulations, approved by Royal Decree

939/2005, of July 29, in relation to article 62 of Law 58/2003, of December 17,

December, through its entry, indicating the NIF of the penalized person and the number of

proceeding that appears in the heading of this document, in the restricted account

nº ES00 0000 0000 0000 0000 0000, opened in the name of the AEPD in the bank

caria CAIXABANK, S.A. Otherwise, it will proceed to its collection in period

executive.

Received the notification and once executed, if the date of execution is

between the 1st and 15th of each month, both inclusive, the term to make the payment

will be until the 20th day of the following month or immediately after, and if

is between the 16th and last day of each month, both inclusive, the term of the payment

It will be valid until the 5th of the second following month or immediately after.

In accordance with the provisions of article 50 of the LOPDGDD, this

Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with article 48.6

of the LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the

Interested parties may optionally file an appeal for reconsideration before the

director of the AEPD within a month from the day following the notification

cation of this resolution or directly contentious-administrative appeal before the

Contentious-administrative Chamber of the National High Court, in accordance with the provisions

placed in article 25 and in section 5 of the fourth additional provision of the Law

29/1998, of July 13, regulating the Contentious-administrative Jurisdiction, in the

period of two months from the day following the notification of this act,

in accordance with the provisions of article 46.1 of the aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of article 90.3 a) of the LPACAP,

the firm resolution may be suspended in administrative proceedings if the interest

sado expresses its intention to file a contentious-administrative appeal. Of being

In this case, the interested party must formally communicate this fact in writing

addressed to the AEPD, presenting it through the Electronic Registry of the Agency

[https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other

records provided for in article 16.4 of the LPACAP. You must also transfer to the

Agency the documentation that proves the effective filing of the contentious appeal

so-administrative. If the Agency was not aware of the filing of the appeal

contentious-administrative within a period of two months from the day following the notification

cation of this resolution, would end the precautionary suspension

Sea Spain Marti

Director of the AEPD

938-26102021