 File No.: EXP202206971

RESOLUTION OF SANCTIONING PROCEDURE

Of the procedure instructed by the Spanish Agency for Data Protection and based on

to the following:

BACKGROUND

FIRST: D.A.A.A. (hereinafter, the claiming party) on May 29,

2022 filed a claim with the Spanish Data Protection Agency. The

The claim is directed against Telefónica Móviles España, S.A.U. with NIF A78923125

(hereinafter, the claimed party or Telefónica Móviles).

The reasons on which the claim is based are the following:

The claimant states that on May 27, 2022, he received a message from

text from the claimed party thanking him for contracting a service that had not

neither requested nor contracted and, immediately afterwards, his telephone line stopped working.

Subsequently, he received several messages from his bank on another telephone line

notifying you of several unauthorized transfers made in your name, for

that your bank had to block both access to your bank account and

to your card.

As a result of what happened, he filed the corresponding complaint with the Police and

went to a store of the claimed party to request a new duplicate of his

SIM card and thus recover your line, but they did not provide you with information about who

requested the previous duplicate or through what means or where it was made.

On June 1, 2022, the complaining party provided a response from Telefónica

Mobiles to your claim, returning the XX.XX euros that the store charged you

Movistar for doubling your sim card in order to recover your line.

Along with the claim, the following relevant documentation is provided:

Screenshot received regarding an order supposedly placed (in details of the

order contains: additional line XL).

List of bank movements and details of controversial transfers.

Screenshots of the personal area of the claimed party.

Copy of the complaint filed with the Police (dated May 27, 2022).

Copy of the claim made (on May 28, 2022) through the forum

Movistar Community.

Copy of the SIM card change contract (dated May 28, 2022) and the

corresponding invoice, as well as a transcript of the conversation held (at

via chat) with the claimed party, on May 29, 2022, in which a

agent indicates, among others, the following: "For you to request a duplicate Sim

You must go to the store with your ID and pay the amount as you already did". The claimant

indicates that the previous duplicate was made without his consent and the agent adds that

"it must have been some Internet hacker" also indicating that "since

This means I can not check in which store the sim has been modified".

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5

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

forward LOPDGDD), said claim was transferred to the claimed party, for

to proceed with its analysis and inform this Agency within a month of the

actions carried out to adapt to the requirements established in the regulations of

Data Protection.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of

October 1, of the Common Administrative Procedure of the Administrations

Public (hereinafter, LPACAP), was collected on July 4, 2022 as

It appears in the acknowledgment of receipt that is in the file.

On August 3, 2022, this Agency received a written response

indicating:

"Prior to the notification of the reference claim, specifically the

May 31, it was received by the service channels for the exercise of rights and

in the mailbox enabled by the office of the Movistar Data Protection Delegate

query on the same matter, presented by the claimant, which is attached,

as attached document No. 1. In order to respond to the aforementioned

claim, was sent to the email address provided by the claimant

an identification request. Such identification request was answered by the

client providing a photocopy of their ID. Both the information request letter

Additional information for the identification of the client, such as the photocopy of the attached DNI, is provided

as attached document No. 2.

In response to the claimant's request, a letter was sent to the address of

email provided by the same, as evidenced by the documentation that is

attached, as annex document no. 3.

Lastly, it should be noted that the Movistar claims department also received

a claim by the claimant that was resolved favorably and that was

answered with the literal that is attached as annex document No. 4.

On 05/27/2022 it is stated that the client contacted our call center

customer service to indicate that your mobile service is not working. Automatically,

the same 05/27/2022 the restriction of the line is applied, with respect to which had been

produced the change of ICC.

On 05/28/2022, there are requests to remove the restriction on the aforementioned line, as well as the ICC duplicate requested by the client. In this way, they have reinforced the different processes, which we will detail in the next point. In relation

with the facts described, this company reports that the facts denounced have already have been treated and solved prior to the entry of the complaint before the Agency. In this regard, we inform you that Telefónica has a procedure consolidated and adequate verification of the identity of our clients that has sufficient guarantees to identify the applicant for the duplicate of SIM card before processing it. However, the above Telefónica works continuously to improve the measures available to it with the objective of avoiding identity theft in the different processes of contracting and subsequent procedures requested by the holders of the services through of the different channels available.

Regarding the amount that you have had to pay for the issuance of a new SIM card, we inform you that the necessary instructions have been given to return that amount. 4.

During 2020, the following specific measures have been implemented that affect the operations of the channels: -Measures adopted in the telephone channel: Referral to the face-to-face channel of those sensitive operations that recommend a additional customer identification (for example, Registration, Mobile Portability and SIM card duplicates). Additionally, the operations are referred to the online channel

modification of personal data such as email and contact telephone number, and a Back Specialized office for requests for change of ownership and change of means of contact for movistar.es credentials. -Measures adopted in the channel face-to-face: Those sensitive operations that advise a additional identification of the client, and for the purposes of guaranteeing compliance with that operational, an additional penalty has been established for the entire face-to-face channel for each procedure carried out and incorrectly documented by a commercial.

In addition, the weekly publication of a report is being carried out in which detail, store by store, certain sensitive operations to check if performs the client identification correctly or not.

Likewise, the "verification call" for authorized persons has been included, which consists of making a prior control call to the line on which the certain sensitive operations, so that the owner client can authorize or not said operation before its execution. As reinforcement, and in support of the previous initiatives, training reinforcements have been carried out for the entire sales network, Doubt sessions, publication of infographics and operational reminders. In that continuous review and improvement process, generally also in 2020 work has been done on the development of a customer authentication system via OTP that serves to reinforce the level of identification of our clients. Said system is is being progressively implemented in the different operations and in the different channels depending on their criticality. Additionally and from the year 2021 We are working on the development of a digital Onboarding of our clients that allows us to have your verified digital identity and biometric authentication on file, which will be implemented to the extent of its availability for the different channels and sensitive operations.

THIRD: On August 19, 2022, in accordance with article 65 of the

LOPDGDD, the claim presented by the claimant party was admitted for processing.

FOURTH: On October 26, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate disciplinary proceedings against the claimed party,

pursuant to the provisions of articles 63 and 64 of the LPACAP, for the alleged

infringement of Article 6.1 of the GDPR, typified in Article 83.5 of the GDPR.

FIFTH: On November 4, 2022, Telefónica Móviles requests the extension

of the legal term granted to formulate allegations, being granted.

SIXTH: Notified the aforementioned start agreement in accordance with the rules established in

the LPACAP, the claimed party submitted a pleading in which, in summary,

manifests, firstly, "prior question of criminal prejudiciality, based on the fact that the

situation described by the complaining party is the consequence of a criminal act

who apparently, with the manifest desire to deceive Telefónica, impersonated

the identity of the claimant, with the ultimate goal of harming the end customer.

In addition, it points out that both the client and Telefónica are harmed in this type of

of situations. Telefónica suffers from it, among others, through the deception that is seen

subjected to our commercials by the impersonators, and in the same way the

client, since he, in addition to "removing the line" to gain control, in

a previous moment, these impersonators must also have the data

bank or financial accounts of the person affected by the fraud.

As the Agency already knows, the detection of this type of practice is done as soon as possible.

possible in the knowledge of the affected distributors so that they can take the necessary measures appropriate and use extreme precautions.

However, it should be borne in mind that such commercials face action of the supplanter who, after obtaining a series of personal data, uses them to promptly process a particular management according to the procedures established for this in Telefónica.

In order for a conduct to be reproached, it is required that it be typical, unlawful and guilty, therefore, and once the facts have been analyzed, this party considers that the principle of typicality is being violated given that the conduct carried out by Telefónica is not subsumable in any of the precepts whose violation is accused.

We remind you that, in this case, the Agency considers that article 6.1 of the GDPR (conditions in which the treatment will be considered lawful) and the infringement typifies it in accordance with article 83.5 GDPR. However, the Agency does not mention about which of the legitimizing bases that are collected in art. 6.1 would be the necessary to carry out the treatment of the data of the claimant who has originated this Agreement, so that it could be understood legitimate. This part understands that the legal basis that legitimizes the processing of the personal data of the claimant cannot be other than the performance of the contract, that is, the basis legitimacy that contemplates section b) of the aforementioned article 6.1: "the treatment is necessary for the performance of a contract to which the interested party is a party or for the application at his request of pre-contractual measures".

In this sense, the Agency has not considered that the treatment is covered by our Privacy Policy as part of data processing

personal information that my client performs under the legitimizing basis of

execution of the contract.

Based on the foregoing, we understand that the imputation to my client of a

infringement of article 6.1 of the GDPR, since the processing of such data by

Telefónica is necessary to manage the contractual relationship with the claimant and,

therefore, Telefónica had a sufficient legal basis.

Finally, this party is interested in pointing out that the consideration of the facts that are the object of the

procedure as unlawful supposes the qualification of the same by the result of

the acts of deception, manipulation and illicit use of the data, carried out by the

possible bank fraudster who could have impersonated the claimant's identity,

not for the actions of my client.

Regarding the graduation criteria of the sanction, this part intends to express its

disagreement with the Agreement, when it provides as a circumstance to aggravate the

sanction the following: "The evident link between the business activity of the

claimed and the processing of personal data of clients or third parties (article

83.2.k, of the RGPD in relation to article 76.2.b, of the LOPDGDD)". As to

this aggravating circumstance raised by the Agency, as it has been exposed in the present

In writing, this party considers that there has not been a

illegitimate processing of the claimant's data, whenever their processing is

is legitimized by article 6.1 of the GDPR, I feel this is necessary for the

execution of a contract to which the interested party is a party.

Therefore, to the extent that this party does not consider that there has been a

illegitimate processing of the claimant's data, we cannot likewise consider

that the aggravating circumstance raised by the Agency in the Agreement concurs.

Likewise, it is interesting to highlight the mitigation considered by the Agency, when indicates that: "The claimed party proceeded to solve the incident object of claim effectively (art. 83.2 c)", and we indicate this in the allegations submitted to the information file of which the present sanction brings cause.

This claim was dealt with prior to the notification of the aforementioned proceedings.

One of the actions taken by Telefónica before receiving the claim was the refund made for an amount of €XX.XX for SIM card change.

Telefónica has proceeded to process the data of the claimant with the diligence due, since the processing of the claimant's data has been carried out with the sufficient legitimizing base and with the necessary security measures that are materialize in the identification protocol followed by this part.

The doctrine of own acts already used by the Courts, in summary, accepts the idea that words and gestures link us, that is, it establishes the inadmissibility of acting against one's own acts done previously; forbids that a person can go against his own behavior shown previously

to limit the rights of another, who had acted in that way moved by the good faith of the first.

In this sense, it is interesting to highlight that the Agency's actions before a file referring to facts substantially the same as those that are the object of claim that concerns us, has been contradictory, as the

own Agency in the file with reference No. EXP202104446 dated 26
January 2022, in which it was filed on the understanding that there had already been
disciplinary proceedings in progress for the same facts, whose literal was the
following: "On this point, it should be noted that facts similar to those that are
object of claim have been investigated by this Agency and penalized in the
disciplinary procedure PS/00021/2021, processed against the claimed party, for
resolution dated 11/8/2021, so the start of a new
disciplinary procedure". Consequently, the performance discrepancy
between one file and another would mean a clear violation of the doctrine
of their own acts and would create palpable legal uncertainty and, consequently,
would suppose the concurrence of the cause of annulment of the Agreement provided for in the
Article 48.1 of Law 39/2015 of October 1, on Administrative Procedure
Common for Public Administrations, hereinafter Law 39/2015. Telefónica has already
been penalized for the same facts that are taking place today in this proceeding,
the Agency imposed the sanction through the procedure with reference
PS/00021/2021, and as the Agency knows, currently, the
corresponding appeal before the Courts of Justice.

The foregoing leads us to consider that initiating a new disciplinary procedure,
successively, without there being a pronouncement by the Courts of
Justice, and on the same facts, violates the non bis in idem principle. How is
Known, the non bis in idem principle prohibits penalizing the same act twice
illicit, since doing so would imply prosecuting and assessing from a legal point of view what
same. In the opinion of this party, this is what the Agency intends in the Agreement,
where it comes to punish "the same": the punishment falls on the same subject, for the
itself and to supposedly protect the same legal right. according to doctrine
consolidated Constitutional Court, the Spanish Constitution prohibits the

Imposition of more than one punishment for the same crime.

For all of the foregoing, I request the Agency, that, considering presenting on time and

form, this brief of allegations, please admit it, and prior to the formalities

opportune, by virtue of: i. The non-existence of responsibility is declared on the part of

Telefónica for the presumed infringements charged against it in this proceeding,

ordering the filing of this disciplinary file. ii. Subsidiarily and for

In the event that this disciplinary file is not filed, the

suspend this procedure and require the claimant to contribute in

what point is the complaint filed, as well as the content of the criminal procedure

that, if applicable, is underway, in order to determine if there is

criminal prejudice. iii. Lastly, if none of the

previous claims, that the penalty initially proposed by virtue of the

art. 83 of the GDPR".

SEVENTH: On November 22, 2022, the instructor of the procedure agreed

perform the following tests: 1. They are considered reproduced for probative purposes the

claim filed by D. A.A.A. and its documentation, the documents obtained

and generated during the phase of admission to processing of the claim. 2.Also, it

considered reproduced for evidentiary purposes, the allegations to the agreement to start the

referenced sanctioning procedure, presented by TELEFÓNICA MÓVILES

ESPAÑA, S.A.U., and the accompanying documentation.

EIGHTH: On January 24, 2023, the proposed resolution was formulated,

proposing that the Director of the Spanish Data Protection Agency

sanctions the defendant, for a violation of Article 6.1 of the GDPR, typified in the

Article 83.5 of the GDPR, with a fine of 70,000 euros.

EIGHTH: Notified of the resolution proposal, on February 1, 2023, requested

Extension of term to formulate allegations, being granted.

The claimed party submitted a written statement confirming those made to the

Initiation Agreement, requesting that this procedure be suspended and that the

claimant in order to provide at what point is the complaint filed, as well as the

content of the criminal procedure that, if applicable, is underway, in order to

to determine if there is criminal prejudiciality, propose a declaration of non-existence of

responsibility on the part of the defendant for the presumed infringement that is imputed to him in

this procedure, and that a Resolution be issued in due course ordering the filing of the

present disciplinary file to the referenced margin, and secondarily, minore

the initially proposed sanction of art. 83 of the GDPR.

Of the actions carried out in this procedure and of the documentation

in the file, the following have been accredited:

PROVEN FACTS

FIRST. - The claiming party filed a claim with this Agency on 29

May 2022 in which it is stated that they have suffered an identity theft

on May 27, 2022, in connection with the obtaining by a third party of a

duplicate of your SIM card, which caused economic damage, since it was

made numerous transfers from his bank account.

SECOND. - It is on record that the claimant on May 27, 2022, at 5:50 p.m. received a

SMS from Movistar informing you that an order had been placed successfully. It was him

order number ***NUMBER.1. This request was never made.

THIRD. - Telefónica certifies that two card changes are recorded in its systems

SIMs made through a partner distributor: on May 27, 2022

***NUMBER.1 Change of

ICC Mobile Line Contract ***TELEPHONE.1

***CONTRACT.1, and on the 28th of the same month and year ***NUMBER.2 Change of ICC

Mobile Line Contract ***TELEPHONE.1 ***CONTRACT.2.

ROOM. - Telefónica certifies that, on May 27, 2022, the claimant

contacted their customer service center to indicate that the

mobile service. Automatically, the same day they applied the line restriction,

with respect to which the ICC change had occurred.

FIFTH. - It is established that on May 28, 2022, Telefónica removed the restriction

of the aforementioned line, as well as the ICC duplicate requested by the client.

FUNDAMENTALS OF LAW

Yo

Competence

In accordance with the powers that article 58.2 of Regulation (EU) 2016/679

(General Data Protection Regulation, hereinafter GDPR), grants each

control authority and as established in articles 47, 48.1, 64.2 and 68.1 of the

Organic Law 3/2018, of December 5, on the Protection of Personal Data and

guarantee of digital rights (hereinafter, LOPDGDD), is competent to

initiate and resolve this procedure the Director of the Spanish Protection Agency

of data.

Likewise, article 63.2 of the LOPDGDD determines that: "Procedures
processed by the Spanish Data Protection Agency will be governed by the provisions
in Regulation (EU) 2016/679, in this organic law, by the provisions
regulations dictated in its development and, insofar as they do not contradict them, with character
subsidiary, by the general rules on administrative procedures."

II

Criminal prejudice

Beforehand, it is necessary to resolve the allegation presented by Telefónica, based on
to the existence of a criminal prejudiciality.

It manifests itself on these facts that are currently being the subject of a
criminal investigation. Considers that, therefore, in application of the principle of
criminal prejudiciality included in article 10 of the Organic Law of the Judiciary,
The matter should not be resolved through administrative channels as long as it is not resolved
through criminal proceedings. This, he manifests, given that the facts declared proven will link
to the Agency regarding a possible disciplinary procedure, in accordance with the provisions
in article 77.4 of Law 39/2015.

It should be noted that art. 77.4 of the LPACAP, states that: "In the
procedures of a sanctioning nature, the facts declared proven by
Firm criminal judicial resolutions will bind the Public Administrations
regarding the sanctioning procedures that substantiate". However, there is
It should be noted that there is no triple identity necessary to apply article 77 of the
LPACAP, (of subject, fact and foundation), between the administrative infraction that
assesses and the possible criminal infraction or infractions that could be derived from the
presumed Preliminary Proceedings carried out by a court. This, because the
offending subject it is obvious that it would not be the same -with respect to the infractions of the
LOPDGDD, the person responsible is Telefónica, while the criminal person responsible for a

eventual crime of usurpation of personality or fraud would be the third that would have been

impersonated the claimant. Nor would the legal basis be the same:

while the legal right protected by the LOPDGDD is the fundamental right to

protection of personal data, the legal right that is protected in criminal types

whose commission would investigate, if necessary, the Investigating Court would be the state

civil, property, etc.

In this sense, the Judgment of the National Court of

04/27/2012 (rec. 78/2010), in whose second Legal Basis the Court

pronounces in the following terms regarding the allegation of the appellant that the AEPD

has infringed article 7 of R.D. 1398/1993 (rule that was in force until the

entry into force of the LPACAP): "In this sense, Art. 7 of Royal Decree

1398/1993, of August 4, on the procedure for the exercise of power

disciplinary action, only provides for the suspension of the administrative procedure

when the effective and real existence of a criminal proceeding is verified, if

considers that identity of subject, fact and legal basis concurs between the

administrative offense and the criminal offense that may correspond.

However, and for the concurrence of a criminal prejudicial action, it is required that this

directly conditions the decision to be taken or that is essential

to resolve, presuppositions that do not concur in the examined case, in which there is

a separation between the facts for which it is sanctioned in the resolution now

appealed and those that the appellant invokes as possible criminal offences. So, and even

have been initiated, in the present case, and due to the facts now in dispute,

also criminal proceedings against the distribution company, the truth is that both the

sanctioning conduct as well as the protected legal right are different in one way and another

(contentious-administrative and criminal). In criminal matters, the protected legal right is

a possible documentary falsification and fraud, and in the administrative sphere, on the other hand, the

power of disposal of your personal data by its owner, so that such

Respondent's objection must be rejected.

In consideration of the foregoing, the issue raised by

Telephone and should be rejected.

II

Breached Obligation

In advance, it is necessary to point out that article 4.1 of the GDPR defines:

“personal data” as “any information about an identified natural person or

identifiable (“the data subject”); An identifiable natural person shall be considered any person

whose identity can be determined, directly or indirectly, in particular by means of

an identifier, such as a name, an identification number, data of

location, an online identifier or one or more elements of identity

physical, physiological, genetic, mental, economic, cultural or social of said person;”

Issuing a duplicate SIM card entails data processing

personal data of its owner since any person will be considered an identifiable natural person

whose identity can be determined, directly or indirectly, in particular by means of

an identifier (article 4.1) of the GDPR).

Therefore, the SIM card identifies a telephone number and this number in turn,

identifies its owner. In this sense, the CJEU Judgment in case C -

101/2001 (Lindqvist) of 6.11.2003, paragraph 24, Rec. 2003 p. I-12971: "The concept of

"personal data" using Article 3(1) of Directive 95/46

includes, according to the definition in Article 2(a) of said

Directive "all information about an identified or identifiable natural person". This

concept includes, without a doubt, the name of a person next to his telephone number or

to other information relating to their working conditions or hobbies”.

In short, both the data processed to issue a duplicate SIM card and the

SIM card (Subscriber Identity Module) that uniquely identifies

to the subscriber in the network, are personal data, and their treatment must be

subject

to data protection regulations.

Well then, the defendant is accused of committing an offense for violation of the

Article 6 of the GDPR, "Legacy of the treatment", which indicates in its section 1 the

cases in which the processing of third-party data is considered lawful:

"1. Processing will only be lawful if at least one of the following is fulfilled

conditions:

a) the interested party gave his consent for the processing of his personal data

for one or more specific purposes;

b) the treatment is necessary for the execution of a contract in which the interested party

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

c) the processing is necessary for compliance with a legal obligation applicable to the

responsible for the treatment;

d) the processing is necessary to protect vital interests of the data subject or of another

Physical person;

e) the treatment is necessary for the fulfillment of a mission carried out in the interest

public or in the exercise of public powers conferred on the data controller;

f) the treatment is necessary for the satisfaction of legitimate interests pursued

by the person in charge of the treatment or by a third party, provided that on said

interests do not outweigh the interests or fundamental rights and freedoms of the

interested party that require the protection of personal data, in particular when the

interested is a child. The provisions of letter f) of the first paragraph shall not apply.

application to processing carried out by public authorities in the exercise of their

functions".

In turn, article 6.1 of the LOPDGDD, indicates, on the treatment of data

based on the consent of the affected party that: "1. In accordance with

provided in article 4.11 of Regulation (EU) 2016/679, it is understood by

consent of the affected any manifestation of free, specific,

informed and unequivocal by which he accepts, either by means of a declaration or

a clear affirmative action, the processing of personal data concerning him (…)".

Classification of the infringement of article 6 of the GDPR

IV.

The violation of article 6 for which the party claimed in the

This resolution is typified in article 83 of the GDPR which, under the

heading "General conditions for the imposition of administrative fines".

"5. Violations of the following provisions will be penalized, in accordance with the

section 2, with administrative fines of a maximum of 20,000,000 EUR or,

in the case of a company, an amount equivalent to a maximum of 4% of the

total annual global business volume of the previous financial year, opting for

the highest amount:

a) The basic principles for the treatment, including the conditions for the

consent in accordance with articles 5,6,7 and 9."

The LOPDGD, for the purposes of the prescription of the infringement, qualifies in its article 72.1

very serious infringement, in this case the limitation period is three years, "b)

The processing of personal data without the fulfillment of any of the conditions of

legality of the treatment established in article 6 of Regulation (EU) 2016/679".

In this case, it is proven that Telefónica Móviles provided a duplicate of

the SIM card of the complaining party to a third party, without their consent and without verifying

the identity of said third party, which has accessed information contained in the

mobile phone, such as bank details, passwords, email address

email and other personal data associated with the terminal. Thus, the defendant, not

verified the personality of the person who requested the duplicate SIM card, did not take the

necessary precautions so that these events do not occur.

Based on the foregoing, in the case analyzed, the

diligence used by the defendant to identify the person who requested

a duplicate SIM card.

In its response, the Respondent acknowledges that the fraudulent duplication occurred

in a physical establishment, but does not provide any evidence of how the

applicant's identity.

Well then, the result was that the defendant issued the SIM card to a third party who did not

he was the owner of the line.

In the explanation provided by the claimed party, it does not indicate which could have

been the specific cause that led to the issuance of the duplicate, beyond

some generic explanations. In any case, Telefónica Móviles has not been able to

certify that for this case the procedure implemented by it was followed

itself, since, if it had done so, the denial of the

duplicate SIM card.

Based on the foregoing, in the case analyzed, the

diligence used by the defendant to identify the person who requested

a duplicate SIM card.

Telefónica cites in its defense a series of resolutions issued by the AEPD,

stating that EXP20210446 was filed on the understanding that

there was already a disciplinary file in progress for the same events and that Telefónica

has already been sanctioned for the same events that are taking place today in this

procedure, the Agency imposed the sanction through the procedure with reference

PS/00021/2021 and therefore violates the non bis idem principle.

In this regard, it should be noted that said procedures were intended to

analyze the procedures followed to manage SIM change requests

by Telefónica, identifying the vulnerabilities that may exist in the

operating procedures implemented, to detect the causes for which

may be producing these cases, as well as finding points of non-compliance,

improvement or adjustment, to determine responsibilities, reduce risks and raise the

security in the processing of the personal data of the affected persons.

The disciplinary procedure PS/00021/2021, processed against the claimed party, was accused him of the violation of article 5.1f), he is not charged with fraud, nor the treatment of data without legitimacy but a lack of guarantees of the security measures that produces a transfer of data to a third party.

In this disciplinary proceeding, the sanction is imposed because Telefónica provided a duplicate of the complaining party's SIM card to a third party, without your consent and without verifying the identity of said third party, and for this reason imputes article 6.1 of the GDPR.

Regarding the responsibility of Telefónica, it should be noted that, in general Telefónica processes the data of its customers under the provisions of article 6.1 b) of the GDPR, as it is considered a necessary treatment for the execution of a contract in which the interested party is a party or for the application at his request of measures pre-contractual In other cases, it bases the legality of the treatment on the bases provided for in article 6.1.a), c), e) and f) of the GDPR.

On the other hand, to complete the scam, it is necessary for a third party to "impersonate the identity" of the owner of the data, to receive the duplicate of the SIM card. Which entails a priori, a treatment outside the principle of legality since a third party is processing data, since it has access to them, without any legal basis, in addition to the violation of other principles such as confidentiality.

For this reason, this is a process where the diligence provided by the operators is essential to avoid this type of scam and violation of the GDPR.

Diligence that translates into the establishment of adequate measures to guarantee that appropriate security measures are implemented and maintained to protect effectively maintain the confidentiality, integrity and availability of all data personnel for which they are responsible, or of those who are in charge of

another responsible.

The Constitutional Court indicated in its Judgment 94/1998, of May 4, that we

We are faced with a fundamental right to data protection by which

guarantees the person control over their data, any personal data, and

about their use and destination, to avoid illegal traffic of the same or harmful to the

dignity and rights of those affected; In this way, the right to protection of

data is configured as a faculty of the citizen to oppose that

certain personal data is used for purposes other than those that justified

its obtaining.

For its part, in Judgment 292/2000, of November 30, it considers it as a

autonomous and independent right that consists of a power of disposition and

control over personal data that empowers the person to decide which of those

data to provide to a third party, be it the State or an individual, or which can this

third party to collect, and which also allows the individual to know who owns that data

personal and for what, being able to oppose that possession or use.

Regarding the conduct of Telefónica, it is considered that it responds to the title of guilt.

As a repository of personal data on a large scale, therefore, accustomed

or dedicated specifically to the management of the personal data of the

customers, you must be especially diligent and careful in your treatment. That is to say,

From the point of view of guilt, we are facing a winnable error, since, with the

application of appropriate technical and organizational measures, these impersonations

of identity could have been avoided.

It is recital 74 of the GDPR that says: "The

responsibility of the data controller for any data processing

personal data made by himself or on his own. In particular, the controller must

be obliged to apply timely and effective measures and must be able to demonstrate the

compliance of processing activities with this Regulation, including the

effectiveness of the measures. Such measures should take into account the nature,

scope, context and purposes of processing, as well as the risk to the rights and

freedoms of natural persons. Likewise, recital 79 says: The protection

of the rights and freedoms of the interested parties, as well as the responsibility of the

controllers and processors, also with regard to the

supervision by the control authorities and the measures adopted by

they require a clear attribution of responsibilities under this

Regulations, including cases in which a controller determines the purposes and

means of processing jointly with other controllers, or in which the

treatment is carried out on behalf of a person in charge".

Based on the available evidence, it is estimated that the conduct

of the claimed party violates article 6.1 of the RGPD being constitutive of the

infringement typified in article 83.5.a) of the aforementioned Regulation 2016/679.

In this sense, Recital 40 of the GDPR states:

"(40) For processing to be lawful, personal data must be processed with the

consent of the interested party or on some other legitimate basis established in accordance

a Law, either in this Regulation or under other Union law

or of the Member States referred to in this Regulation, including the

the need to comply with the legal obligation applicable to the data controller or the

need to execute a contract to which the interested party is a party or for the purpose of

take measures at the request of the interested party prior to the conclusion of a

contract."

V

Sanction

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

14/17

The determination of the sanction that should be imposed in the present case requires

observe the provisions of articles 83.1 and 2 of the GDPR, precepts that,

respectively, provide the following:

"1. Each control authority will guarantee that the imposition of fines

administrative proceedings under this article for violations of this

Regulations indicated in sections 4, 9 and 6 are in each individual case

effective, proportionate and dissuasive."

"2. Administrative fines will be imposed, depending on the circumstances of each

individual case, in addition to or in lieu of the measures contemplated in

Article 58, paragraph 2, letters a) to h) and j). When deciding to impose a fine

administration 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

such as the number of interested parties affected and the level of damages that

have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor to

alleviate the damages and losses suffered by the interested parties;

d) the degree of responsibility of the controller or processor,

taking into account the technical or organizational measures that they have applied under

of articles 25 and 32;

e) any previous infringement committed by the controller or processor;

f) the degree of cooperation with the supervisory authority in order to remedy 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 whether the person in charge or the person in charge notified the infringement and, if so, in 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 relation to the

same matter, compliance with said measures;

j) adherence to codes of conduct under article 40 or to mechanisms of

certification approved in accordance with article 42, and

k) any other aggravating or mitigating factor applicable to the circumstances of the case,

such as financial benefits obtained or losses avoided, directly or

indirectly, through the infringement."

Within this section, the LOPDGDD contemplates in its article 76, entitled

"Sanctions and corrective measures":

"1. The sanctions provided for in sections 4, 5 and 6 of article 83 of the Regulation

(UE) 2016/679 will be applied taking into account the graduation criteria

established in section 2 of said article.

2. In accordance with the provisions of article 83.2.k) of Regulation (EU) 2016/679

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 data processing.

personal information.

c) The benefits obtained as a consequence of the commission of the infraction.

d) The possibility that the conduct of the affected party could have led to the commission

of the offence.

e) The existence of a merger by absorption process subsequent to the commission of the

violation, which cannot be attributed to the absorbing entity.

f) The affectation of the rights of minors.

g) Have, when it is not mandatory, a data protection delegate.

h) Submission by the person responsible or in charge, on a voluntary basis, to

alternative conflict resolution mechanisms, in those cases in which

there are controversies between those and any interested party.

3. It will be possible, complementary or alternatively, the adoption, when appropriate, of

the remaining corrective measures referred to in article 83.2 of the Regulation

(EU) 2016/679."

In accordance with the precepts transcribed, for the purpose of setting the amount of the sanction of

fine to be imposed on the entity claimed as responsible for a classified offense

in article 83.5.a) of the GDPR and 72.1 b) of the LOPDGDD, are considered concurrent in

the present case the following factors:

As aggravating factors:

-

The evident link between the business activity of the defendant and the

treatment of personal data of clients or third parties (article 83.2.k, of the

GDPR in relation to article 76.2.b, of the LOPDGDD).

The Judgment of the National Court of 10/17/2007 (rec. 63/2006), in which,

with respect to entities whose activity entails the continuous processing of

customer data, indicates that "...the Supreme Court has understood that

recklessness exists whenever a legal duty of care is neglected, that is

that is, when the offender does not behave with the required diligence. And in the

assessment of the degree of diligence, special consideration must be given to the

professionalism or not of the subject, and there is no doubt that, in the case now

examined, when the appellant's activity is constant and abundant

handling of personal data must insist on rigor and exquisite

Be careful to comply with the legal provisions in this regard."

As mitigations:

The claimed party proceeded to block the line as soon as it became aware of the

facts (art. 83.2 c).

It is appropriate to graduate the sanction to be imposed on the defendant and set it at the amount of 70,000

€ for the alleged violation of article 6.1) typified in article 83.5.a) of the

cited GDPR.

Therefore, in accordance with the applicable legislation and assessed the criteria of

graduation of sanctions whose existence has been accredited, the Director of the

Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE TELEFÓNICA MÓVILES ESPAÑA, S.A.U., with NIF

A78923125, for a violation of Article 6.1 of the GDPR, typified in Article 83.5

of the GDPR, a fine of 70,000 euros (seventy thousand euros).

SECOND: NOTIFY this resolution to TELEFÓNICA MÓVILES ESPAÑA,

S.A.U.

THIRD: Warn the penalized person that they must make the imposed sanction effective

Once this resolution is enforceable, in accordance with the provisions of Article

art. 98.1.b) of the LPACAP, within the voluntary payment period established in art. 68 of the

General Collection Regulations, approved by Royal Decree 939/2005, of 29

July, in relation to art. 62 of Law 58/2003, of December 17, through its

income, indicating the NIF of the sanctioned and the number of the procedure that appears in

the heading of this document, in the restricted account IBAN number: ES00-0000-

0000-0000-0000-0000, opened in the name of the Spanish Agency for the Protection of

Data in the banking entity CAIXABANK, S.A.. Otherwise, it will proceed to its

collection in executive period.

Once the notification has been received and once executed, if the execution date is

between the 1st and 15th of each month, both inclusive, the term to make the payment

voluntary will be until the 20th day of the following or immediately following business month, and if

between the 16th and the last day of each month, both inclusive, the payment term

It will be until the 5th of the second following or immediately following business month.

In accordance with the provisions of article 50 of the LOPDGDD, this

Resolution will be made public once the interested parties have been notified.

Against this resolution, which puts an end to the administrative process in accordance with art. 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 reversal before the
Director of the Spanish Agency for Data Protection within a period of one month from
count from the day following the notification of this resolution or directly
contentious-administrative appeal before the Contentious-administrative Chamber of the
National Court, in accordance with the provisions of article 25 and section 5 of

the fourth additional provision of Law 29/1998, of July 13, regulating the
Contentious-administrative jurisdiction, within a period of two months from the
day following the notification of this act, as provided for in article 46.1 of the
referred Law.
Finally, it is noted that in accordance with the provisions of art. 90.3 a) of the LPACAP,
may provisionally suspend the firm resolution in administrative proceedings if the
The interested party expresses his intention to file a contentious-administrative appeal.
If this is the case, the interested party must formally communicate this fact through
writing addressed to the Spanish Data Protection Agency, presenting it through
of the Electronic Registry of the Agency [https://sedeagpd.gob.es/sede-electronica-
web/], or through any of the other registries provided for in art. 16.4 of the
aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the
documentation proving the effective filing of the contentious appeal-
administrative. If the Agency was not aware of the filing of the appeal
contentious-administrative proceedings within a period of two months from the day following the
Notification of this resolution would terminate the precautionary suspension.

Mar Spain Marti

Director of the Spanish Data Protection Agency

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es