 File No.: EXP202204288

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., on behalf of Mrs. B.B.B. (hereinafter, the complaining party) on March 10, 2022 filed a claim with the Spanish Data Protection Agency. The claim is directed against ORANGE ESPAGNE, S.A.U. with NIF A82009812 (hereinafter, the claimed party or Orange).

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

The company "Telecomunicaciones y Energías Renovables R2I, S.L" signed a telephone contract with the claimed entity, the claimant being a worker and proxy of said company, as well as user of one of the telephone lines contracted mobile. It states that, as of January 17, 2022, its mobile line ***TELEPHONE.1 was left without coverage, due to said incident because the Respondent entity provided a third party with a duplicate of the SIM card for said line mobile, without the consent of the company that owns the line, or the user (complainant).

As a result of the information contained in the mobile phone, said third party accessed the electronic banking, making fraudulent transfers from the account of the company, as well as from the personal account of the claimant (on the 17th and January 18, 2022). After what happened, the claimant (through her lawyer) requested to the unsuccessfully claimed entity to provide a copy of the recording relating to the request for the disputed duplicate, as well as the documentation that was delivered by the third party when making the request in the establishment involved,

said entity proceeding to close the claims, alluding to the regulations of

Data Protection.

Likewise, he filed a complaint with the Police, on January 18, 2022,

initiating the corresponding preliminary proceedings.

On the other hand, he states that, in order to recover the line, he had to request a new

duplicate of the SIM card and, in the invoice corresponding to the month of January 2022,

there is a money refund for "SIM change", a refund that was not requested

by the claimant, for what it considers to be a way of recognizing, the entity

claimed, their responsibility for what happened.

It requests this Agency to require the claimed entity to provide the

recording of the request for the duplicate and the documentation that was provided for the

delivery of said duplicate.

And, among other things, it provides the following relevant documentation:

Complaint filed with the Police and extension of the same dated January 18 and

February 4, 20223, indicating that the duplicate of the card was made on February 14,

January 2022 around 7:00 p.m., according to the information provided to the claimant by

Orange customer service on January 19 of the same year.

Telephone bill, in the name of the company, dated February 5, 2022.

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 April 27, 2022 as stated

in the acknowledgment of receipt in the file.

On May 27, 2022, this Agency received a written response

indicating: "that the duplicate e-SIM was detected usurping the identity of the

claimant. The perpetrators of the identity theft contacted a

employee of the Point of Sale of the establishment of TIENDA ORANGE SALT Centro

Commercial ESPAI GIRONES posing as an employee of another Point of

Sale (specifically from an employee of the Phone House on Calle Juan de Austria),

making use of the jargon and lingo of the same, demonstrating knowledge

information on the uses and characteristics of the databases of this company. After

this, due to a completely involuntary error of the Point of Sale Agent and, skipping the

specifications indicated in this type of situation by this company, facilitated the

the claimant's data, understanding that she was speaking with a colleague from another

establishment.

Once the aforementioned data was obtained, it was when this person requested the duplicate e-SIM

submitted by the claimant. By the time the claimant realized that

this circumstance contacted this company, proceeding to block

the line, as well as to make the pertinent adjustments. In this regard, it should be noted that,

In no case have security systems been affected or compromised.

the information of the company, which have not suffered a breach in its operation.

This Agency should be informed of the additional measures that, due to the study

carried out, have been carried out by the company. First, indicate

that this company requested on January 27, 2022 a review of the

inventory at the Point of Sale where the duplicate was made, indicating that they should

Block those SIMs that were not located. Also, from the study conducted

it has been detected that the duplicate was made through an "On Call" service

available in some sales channels available to process registrations when they have

incidents. At present, training in this sense has been reinforced, as well as

indications about SIM duplicates, which is why operations of this

nature, it is no longer possible to request and perform them through this channel. Given

account of what happened in this case, a statement has been issued

to the channel to reinforce the training of agents in this regard. It is contributed as

annex document no. 1 the communication sent.

In the same way, and in collaboration with the authorities, the company has

proceeded to track the IMEI of the device from which the duplicate was made

fraudulent eSIM, including it in the internal BlackList, so that it cannot

be used again.

Lastly, it should be noted that the response of this company to the case at hand was

very agile, immediate, because as soon as the claimant informs the staff

of Orange what happened, the company proceeded to annul the irregular duplicate, to

carrying out all the corresponding adjustments as it has been exposed in

your claim and launched the exhaustive investigation previously

exposed in order to determine the scope of said incident and the root cause that
caused this incident. The claimant was informed of all of the above given that
he continues to be active in this business".

THIRD: On June 1, 2022, in accordance with article 65 of the
LOPDGDD, the claim presented by the claimant party was admitted for processing.

FOURTH: On September 23, 2022, the Director of the Spanish Agency
of Data Protection agreed to initiate disciplinary proceedings against the claimed party,
in accordance with the provisions of articles 63 and 64 of Law 39/2015, of October 1,
of the Common Administrative Procedure of Public Administrations (in
hereinafter, LPACAP), for the alleged infringement of Article 6.1 of the GDPR, typified in
Article 83.5 of the GDPR.

FIFTH: Notified of the aforementioned start-up agreement in accordance with the rules established in
Law 39/2015, of October 1, on the Common Administrative Procedure of
Public Administrations (hereinafter, LPACAP), the claimed party requested
extension of the period to make allegations for five business days, and dated 18
of October 2022, presented a brief of allegations in which, in summary,
manifested
their disagreement with the content of the grounds set forth in the Agreement of
Initiation and the legal allegations and arguments are ratified and considered reproduced
of his previous writing, and states: "that on January 18, 2022 there is a
application to issue a duplicate SIM card. It is produced through
"Atención al Canal", a support service for employees and agents of the
Orange outlets. Thus, the incidence is due to a specific human error.
The Orange Fraud department identifies a breach of the
established protocol (request through the "On Call" tool) in the process of
activation of duplicate SIM card in question. For this reason, he submits himself to a

verification process, so that the process of requesting and granting

the same.

While the Orange Fraud department is in the process of verifying the

SIM duplicate request, the "Claimant", contacts this party

to report that you have been the victim of identity theft.

Immediately, from the Fraud department, the categorization of the

duplicate SIM as irregular, proceeding immediately to block the line.

In collaboration with the authorities, Orange has proceeded to track the IMEI

of the device from which the fraudulent SIM duplicate was made, identifying the

itself and including it in an internal BlackList, so that it can no longer be

used.

Although until now the identity of Orange customers was impersonated, now we see

how he proceeds to impersonate Orange employees and agents. It is therefore

that, faced with the establishment by criminals of new ways and techniques of

commission of fraud, Orange will again proceed to establish protocols and

additional security measures. That is why it is not possible to appreciate

Orange's guilt in the present factual assumption, not being legally

valid the appreciation made by the Agency of commission of infringement for this

trade.

In response to the commission of fraud such as the one at hand, Orange has put into

an action plan is underway that it estimates to have implemented by the end of this year, with the

objective of mitigating the commission of fraud in SIM duplicate processes through

through methods such as “Sim Swapping”. The planned actions are specified

in the following measures: - Implementation of a double identification factor, whose

Pilot project is already active, being in the testing phase with certain users.

- "Whitelist IP" project to limit access to internal Orange systems from

Unidentified IPs. In attention to all the measures stated, consider this

party that has been accredited, by Orange, the use of a level of diligence

suitable with which, although it is not possible, due to limited technology and

human means, the existence of a zero risk, if it is updated and reviewed

periodically in accordance with the state of the art, the application costs, and the

nature, scope, context and purposes of processing, as well as risks of

variable probability and severity for the rights and freedoms of individuals

physical.

Thus, the present assumption is analogous to that included in EXP202104010 to Orange,

also for an alleged fraud 'Sim Swapping', which was filed by the

AEPD.

In this regard, it should be noted that facts similar to those that are the object of

claim have been investigated by this Agency and sanctioned in the

disciplinary procedure PS/00022/2021, processed against the claimed party, for

resolution dated 11/10/2021, so the start of a new

disciplinary procedure”. Each and every one of the elements identified by the

AEPD as archive reasons in this EXP202104010 are reproduced and are

fully applicable to this procedure 202204288. However, the

file identified does not constitute an isolated case. The EXP202104011, also with

in relation to a case of Sim Swapping and also archived by the AEPD to Orange,

indicates, identically: "it should be noted that facts similar to those that are the object of

of claim have been investigated by this Agency and sanctioned in the

disciplinary procedure PS/00022/2021, processed against the claimed party, for

resolution dated 11/10/2021, so the start of a new

disciplinary procedure". And, again and in the same sense, in the

EXP202105686 to Orange, also related to a case of 'Sim Swapping',

proceeds to its file by the AEPD: "In this regard, it should be noted that the

facts claimed refer to the same operating procedure for the protection of

data that has been investigated and sanctioned by the AEPD by resolution dated

11/10/2021 in the framework of the disciplinary procedure PS/00022/2021, processed

against the claimed party, and which will be published on the website www.aepd.es. […]In

this case, after analyzing the reasons given by ORANGE ESPAGNE,

S.A.U., which are in the file, it is considered that the initiation of a

disciplinary procedure after the claim has been dealt with, proceeding

agree to file the examined claim". That is why it is not possible in

the present the imputation of an infraction to this part, when in supposed

manifestly equivalent, an archive criterion has been adopted.

For all of the above, Orange: REQUESTS the Spanish Agency for Data Protection

that this document is considered as presented, if it is admitted, considers as formulated the

previous allegations and, after the appropriate procedures, issue a resolution through

which points to the file. Secondarily, in the event that the AEPD resolves in

against the legal grounds that Orange maintains, the AEPD is requested to

take into account extenuating circumstances based on the above

allegations and, consequently, conclude the procedure by means of a

warning and, ultimately, if it considers that the imposition of a

sanction, moderate or modulate its proposal included in the Commencement Agreement notified to

Orange, based on the arguments expressed in the body of this document

of allegations".

SIXTH: On October 19, 2022, the procedure instructor agreed

perform the following tests:

"1. The claim filed by the

claimant and its documentation, the documents obtained and generated during the

phase of admission to processing of the claim. 2. Likewise, it is considered reproduced at

probative effects, the allegations to the agreement to start the procedure

referenced sanctioner, presented by Orange., and the documentation that they

accompanies".

SEVENTH: On November 15, 2022, Orange was notified of the Proposal for

Resolution, by which it is proposed to penalize Orange for alleged infringement of the

Article 6.1) of the GDPR, typified in Article 83.5.a) of the GDPR.

EIGHTH: Once the proposed resolution was notified, the defendant requested an extension

of the term to formulate allegations for five business days, and dated December 7

of 2022, he presented a brief of allegations in which, in summary, he stated his

disagreement with the content of the grounds set forth in the Proposal for

Resolution and the allegations and arguments are ratified and reproduced

of his previous writing, and states:

"The AEPD begins its rationale by reiterating the forced interpretation that the

SIM card not only contains, but also constitutes, in itself, data of a personal nature.

staff.

While this part acknowledges that the process of issuing a duplicate SIM card involves the processing of data, it must be pointed out that the data that supposedly make the SIM card personal data for the AEPD are: • The MSISDN is the number telephone number of the owner of the line (preceded by the national prefix). As is evident to Under the assumption of fact, the alleged impersonators already knew the telephone number of the owner of the line prior to having contact with ORANGE, as long as it was provided by them when requesting a duplicate SIM card. • The IMSI is technical information that identifies the subscriber on the line, but only to your telephone company, which has sufficient information to relate it to its owner. For anyone who does not have access to the systems of the telephone company (in this case ORANGE), it is not possible to relate this data with a specific person. In addition to the above, it is especially relevant is a fact that the AEPD has overlooked and that is that the subscriber is, in this case, a legal person.

Therefore, even in the totally improbable event that a third party could arrive to relate the data contained in the card with a subscriber, the truth is that it is not would identify a natural person, but rather a company, which is the owner of the line: in Specifically, the company “Telecomunicaciones y Energías Renovables R2l”, S.L. This mercantile is the entity that has contracted with ORANGE, being its only client in the present assumption.

That is to say, that both the telephone number and the IMSI affected in the present

As a matter of fact, they are outside the definition of personal data made by the

article 4 of the GDPR. Thus, said treatment would be outside the scope of application of

personal data protection regulations and, consequently, outside the scope

of action of the control authority. All this, also taking into account that it is

evident that the identity theft knew of and had under his control – in a manner

prior to any contact with ORANGE - the data of the impersonated telephone line.

This information, obtained before contacting ORANGE, is what has allowed us to

the impersonator managed to gain access to a duplicate of the SIM card of the

trade. Therefore, beyond the theoretical conceptualization of the data included in

a SIM card as personal data, it has not been proven that it was produced,

in this case, a processing of personal data.

It is a fact that banks are solely responsible for security

of its operations, as stated by the European Banking Authority (hereinafter,

the “EBA”) in the following pronouncements: • Opinion on the implementation of the

RTS on SCA and CSC: in its section regarding who decides on the means to

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

used to perform secure authentication of the users of the

payment services are the responsibility of the account services management entity (in

the case at hand, financial institutions). • Qualification of SMS OTP as an

authentication factor | European Banking Authority: indicates that the use of SMS

ordinary is not feasible for the confirmation of banking operations, for not being

sufficiently safe according to the standards of Directive (EU) 2015/2366 of the

European Parliament and of the Council of November 25, 2015 on information services

payment in the internal market (PSD2). In this sense, it indicates that: "article 22 (1) of the

Regulation requires that 'payment service providers shall guarantee the

confidentiality and integrity of the user's personalized security credentials

payment service user, including authentication codes, during all

phases of authentication' and article 22, paragraph 4, of the Delegated Regulation

establishes that 'payment service providers shall ensure that the

processing and routing of personalized security credentials and

of the authentication codes generated in accordance with Chapter II have

take place in secure environments consistent with strong standards and widely

recognized in the sector. The bold corresponds to this part. Therefore it is

Undoubtedly, the payment service provider is subject to compliance

of specific protection obligations in the authentication processes of the

payment operations whose purpose is to minimize the probability of execution of

unauthorized operations, but in no case prevent them from occurring. Of

In this way, the assumption of fact would remain in accordance with the provisions of the regime provided for in the

Royal Decree-Law 19/2018, of November 23, on Payment Services and other Measures

Urgent in financial matters, and the responsibility of the provider must be assessed

of payment services.

Thus, it contradicts any legal logic to transfer all responsibility to the entity

that provides telephone services, being the mere communication channel

selected by the financial institution itself and without it being aware of it, in

any, that the data transmitted through the messages sent contain

Banking keys. Extrapolating the factual assumption to others

environments, it would be unheard of to hold accountable entities that allow the creation of

email accounts, such as Google or Yahoo, that a

identity theft through a "phishing" attack, using the attacker the

email as a means to carry out the subsequent fraudulent operation.

Note that ORANGE does not offer online trust services to operators

nor does it offer the services of a certification entity or

accreditation. Banking entities may not have contracted any service to

ORANGE, and, even so, use SMS to carry out their actions with

customers. Therefore, ORANGE cannot be held responsible for the configuration of the

sending SMS as a second authentication factor used by those responsible for

other services, such as bank operators. It's totally inappropriate

claim that, if the banking entities decide to trust the identification made

by third parties, they are held responsible for such a decision, unless they provide this type of

services, in accordance with those established in Regulation (EU) No. 910/2014 of the

European Parliament and of the Council, of July 23, 2014, regarding the identification

electronics and trust services for electronic transactions. and not this

This is the case of the services provided by ORANGE.

ORANGE cannot take charge of the security of third-party operations

entities for the mere fact that they use telecommunications services. This

This fact is even more evident in the present case, since it must be reiterated that,

although it may have been affected by the impersonation of the SIM card request

a natural person, the owner of the telephone line affected by the impersonation and the

fraud SIM SWAPPING is a legal entity, therefore there is no relationship

connection between the identity of the natural person and the supposed supplanting of the telephone line

telephone.

In this sense, the AEPD ignores the fact that ORANGE has prepared and implemented a SIM card duplicate request protocol, and communicated to the agents in charge of processing these requests. Not included slightest consideration about its content or its adequacy for evaluate the display of diligence that ORANGE has undertaken. The fact that the protocol has not been followed implies a breach of contract by the agent of the collaborating entity, sanctioned by ORANGE (which does not have legal capacity to act directly against the agent, so it is directed against your employer). In this sense, the alleged personification of ORANGE, as if the entity materially performed some action. It is obvious that the legal persons act through their representatives, employees and collaborators and that they are the ones who must comply in the exercise of their functions with established protocols. In this case, as has been proven, the The entity has an adequate protocol for the correct processing of the applications (whose effectiveness in preventing fraud is very high, exceeding the 99%). In this case, the impersonation derives from the inappropriate performance of one of the agents. In this sense, it must be taken into consideration that it is not feasible to elimination of the risk associated with the human factor, since non-compliance with the established procedures is not materially avoidable, unless it is dispensed with human intervention in the entire contracting process, which, apart from being unfeasible, would imply fully automated decision-making, which is considered as a risk by the GDPR itself.

It is worth reminding the Agency, which is the Constitutional Court (hereinafter, TC),

which, since its Judgment No. 76/1990 of April 26, has been warning of the
problem of inadmissibility in our legal system of liability
objective and, consequently, the requirement in any case that the Administration,
When sanctioning, try some degree of intentionality in the sanctioned. In the
indicated sentence, it was pointed out that the possibility of imposing a sanction requires
the concurrence of guilt in the degrees of fraud and gross negligence or negligence, not
mere negligence being enough. For this reason, the possibility of
penalize for the mere occurrence of a result, understanding the TC that "the mere
Human error cannot give rise, by itself (and especially when it occurs with
isolated character), to the attribution of penalizing consequences; well, to be done
thus, it would incur in a system of strict liability prohibited by our order
constitutional". By virtue of the foregoing, it is possible to affirm that this procedure,
used in the current AEPD Proposal, which associates mere human error
penalizing consequences, is not in accordance with the law, as has already been
also indicated by the National Court, among others, in its Judgment of the Chamber of
Administrative Litigation, Section 1, of December 23, 2013, Rec.
341/2012.

It is true that there are protocols to prevent identity theft in
these processes; that those involved in the processing have been transferred; that have
introduced improvements after discovering certain vulnerabilities; that there are penalties
for its breach. However, we do not share the fact that these protocols
or internal procedures may be considered adequate insofar as they are
susceptible to improvement. Mechanisms for identifying and
authentication with technical and organizational measures that are especially
appropriate to avoid impersonation. Regarding due diligence, it is recognized

that ORANGE has acted diligently in minimizing the impact to

potentially affected by implementing new security measures to avoid repetition

of similar incidents in the future. That is, the existence of the

ORANGE protocols and the introduction of improvements and new measures to

increase its effectiveness, as well as the diligence of ORANGE in minimizing the

impact and implementation of the protocols, however, it qualifies them as

not adequate, as "they are susceptible to improvement".

For all of the above, ORANGE: REQUESTS the Spanish Agency for the Protection of

Data that this writing considers to be presented, serve to admit it, consider

formulated the previous allegations and, after the appropriate procedures, issue

resolution by means of which the file of Procedure No. is indicated:

PS/04288/2022. Secondarily, in the event that the AEPD decides against

the legal foundation that ORANGE maintains, the AEPD is requested to take into account

account the extenuating circumstances based on the above allegations and,

consequently, culminate the procedure by means of a warning and, ultimately,

instance, if it considers that the imposition of a sanction is appropriate, moderate or modulate its

proposal included in the Sanction Proposal notified to ORANGE”

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

in the file, the following have been accredited:

PROVEN FACTS

FIRST: The claimant states that, on January 17, 2022, he ran out of

coverage on your mobile line ***TELEPHONE.1, obeying said incident to the fact that the

Respondent entity provided a third party with a duplicate of the SIM card for said line mobile, without the consent of the company that owns the line, or the user (complainant).

SECOND: The claimant has provided a copy of the complaint filed before the Police and its extension dated January 18 and February 14, 2023, stating that the duplicate of the card was made on January 14, 2022 on the 7:00 p.m., according to information provided to the claimant by the customer service Orange customer on January 19 of the same year.

THIRD: Orange acknowledged both in the response brief dated May 27, as in the one of allegations of October 18, 2022 to this Agency that the incidence is due to a specific human error, by the Agent of the Point of Sale of Orange "that on January 18, 2022, a request is made to issue a duplicate of SIM card. It is produced through "Atención al Canal", a service of support for employees and agents of Orange points of sale. So, the incidence is due to a specific human error".

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

Classification and classification of the offense

Article 4 of the GDPR, under the heading "Definitions", provides the following:

"1) «personal data»: 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;

2) "processing": any operation or set of operations carried out on personal data or sets of personal data, either by procedures automated 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, deletion or destruction".

7) "responsible for the treatment" or "responsible": the natural or legal person, public authority, service or other body which, alone or jointly with others, determines the

purposes and means of processing; if the law of the Union or of the Member States

determines the purposes and means of processing, the controller or the

Specific criteria for their appointment may be established by Union law

or of the Member States”

ORANGE, is responsible for the data processing referred to in the

exposed background, since according to the definition of article 4.7 of the

GDPR is the one that determines the purpose and means of the treatments carried out with the

purposes indicated in its Privacy Policy.

Likewise, the issuance of a duplicate SIM card supposes the treatment of the data

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

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

using an identifier (article 4.1) of the GDPR).

In Spain, since 2007, through the Sole Additional Provision of the Law

25/2007, of October 18, on the conservation of data related to communications

electronic networks and public communications networks, it is required that the holders of

all SIM cards, whether prepaid or contract, are duly

identified and registered. This is important since the identification of the subscriber

It will be essential to register the SIM card, which will mean that when

obtain a duplicate of this the person who requests it has to identify himself

equally and that their identity coincides with that of the owner.

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.

The defendant is accused of committing an infraction for violation of article 6

of the RGPD, "Legacy of the treatment", which indicates in its section 1 the assumptions in which

that the processing of data by third parties 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".

The infringement is typified in article 83.5 of the GDPR, which considers as such:

"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 LOPDGDD, 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>>

II

Breached Obligation

In response to the allegations presented by the respondent entity, it should be noted

the next:

Regarding the fact that the issuance of a duplicate is not enough to carry out operations

bank accounts on behalf of the holders, certainly, to complete the scam, it is

necessary for a third party to "supplant the identity" of the owner of the data before the entity

financial. What entails a priori, a treatment outside the principle of legality

because a third party is 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 the data processing is in accordance with the GDPR.

Identical considerations deserve the actions of banking entities that

provide payment services, in which area this type of scam starts, since

the third party has access to the affected user's credentials and poses as

this.

While these entities are responsible for the processing of the data of their

customers, they are responsible for the same obligations as those indicated up to now for the

operators referring to compliance with the RGPD and the LOPDGDD, and also the

derived from Royal Decree-Law 19/2018, of November 23, on payment services and

other urgent financial measures.

From the Proven Facts, it can be deduced that ORANGE has provided a duplicate card

SIM to a third party other than the legitimate holder of the mobile line, after overcoming by

third person of the existing security policy, which shows a

breach of duty to protect customer information.

This unauthorized access to the personal data of those affected is

determinant for the subsequent actions developed by the people

impersonators, since they take advantage of the space of time that elapses until the

The user detects the failure on the line, contacts the operator, and the latter

detects the problem, to carry out fraudulent banking operations and that without the

duplicate SIM card would have become impossible.

Denying the concurrence of a negligent act on the part of ORANGE would amount to

to recognize that his conduct -by action or omission- has been diligent. Obviously not

We share this perspective of the facts, since the

lack of due diligence. It is very illustrative, the SAN of October 17, 2007

(rec. 63/2006), assuming that these are entities whose activity involves

in continuous treatment of customer data, indicates that "...the Supreme Court comes

understanding that imprudence exists whenever a legal duty of

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

assessment of the degree of diligence, professionalism must be especially considered

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

The appellant's activity is constant and abundant handling of personal data.

staff

must insist on the rigor and exquisite care to adjust to the

legal provisions in this regard.

It is proven in the file that security has not been guaranteed

appropriate in the processing of personal data, taking into account the result that

identity theft has occurred. That is, a third party has managed to access

to the personal data of the owner of the line without the security measures that

ORANGE affirms that they exist, they have been able to prevent it. So, we are before the

concurrence of a typical conduct, unlawful and guilty.

In short, the rigor of the operator when monitoring who owns the

SIM card or person authorized by it who requests the duplicate, should

meet strict requirements. It is not that the information to which

refers is not contained in the SIM card, but that, if in the process of issuing

of a duplicate SIM card does not properly verify the identity of the

applicant, the operator would be facilitating identity theft.

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

stating that the present case is analogous to that included in the

procedures EXP202104010; EXP202104011 and EXP202105686 to ORANGE,

also for cases of "Sim Swapping" fraud, which were filed

by the AEPD.

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

analyze the procedures followed to manage SIM change requests

by ORANGE, 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

facts claimed, in the aforementioned procedures, refer to the same procedure

data protection operation that has been investigated and sanctioned by the AEPD

by resolution dated 11/10/2021 within the framework of the disciplinary procedure

PS/00022/2021, processed against the claimed party and charged with the violation of the

article 5.1f).

In this disciplinary proceeding, the sanction is imposed because

ORANGE provided a duplicate SIM card of the complaining party 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.

In the case now examined, the AEPD, after carrying out the investigations timely, and in relation to a series of specific facts that it considers proven, includes them in the infringing type that it considers appropriate, in accordance with the application and interpretation of the regulations, motivating in a neat and sufficient way such performance. And it is that, the AEPD is bound by the principle of legality that implies the application and interpretation of the rules taking into account the assumption of fact specific to each case.

Regarding ORANGE's responsibility, it should be noted that, in general ORANGE 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.

As for ORANGE's conduct, it is considered to respond 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".

The computer system and the technologies involved must be adequate for

prevent spoofing and be correctly configured.

This Agency does not share ORANGE's statements regarding the

circumstances that have been proven.

It is true that there are protocols to prevent identity theft in these

processes; that those involved in the processing have been transferred; that have

introduced improvements after discovering certain vulnerabilities; that there are penalties

for its breach. However, we do not share the fact that these protocols

or internal procedures may be considered adequate insofar as they are

susceptible to improvement. Mechanisms for identifying and

authentication with technical and organizational measures that are especially

appropriate to avoid impersonation.

Regarding due diligence, it is recognized that ORANGE has acted

diligently in minimizing the impact on those potentially affected by implementing

new security measures to avoid the repetition of similar incidents in a

future.

Certainly, the principle of responsibility provided for in article 28 of the LRJSP,

provides that: "They may only be penalized for acts constituting an infringement

administrative authority for natural and legal persons, as well as when a Law

recognize capacity to act, affected groups, unions and entities without

legal personality and independent or autonomous estates, which result

responsible for them by way of fraud or negligence.”

However, the mode of attribution of liability to legal persons is not

corresponds to the willful or reckless forms of guilt that are imputable

to human behavior. So, in the case of offenses committed by

legal persons, even if the element of guilt must be present, it will be

necessarily applies differently from what is done with respect to persons

physical.

According to STC 246/1991 "(...) this different construction of the imputability of the

authorship of the infraction to the legal person arises from the very nature of fiction

law to which these subjects respond. The volitional element is lacking in them in the sense

strict, but not the ability to break the rules to which they are subject.

Infringement capacity and, therefore, direct reproach that derives from the good

protected by the rule being infringed and the need for such protection

is really effective and because of the risk that, consequently, the person must assume

that is subject to compliance with said standard" (in this sense STS of 24

November 2011, Rec 258/2009).

To the foregoing must be added, following the judgment of January 23, 1998,

partially transcribed in the SSTS of October 9, 2009, Rec 5285/2005, and of 23

of October 2010, Rec 1067/2006, that "although the guilt of the conduct must

also be the object of proof, must be considered in order to assume the

corresponding charge, which ordinarily the volitional and cognitive elements

necessary to appreciate it are part of the typical behavior tested, and that its

exclusion requires that the absence of such elements be proven, or in its aspect

regulations, that the diligence that was required by the person claiming their

nonexistence; In short, it is not enough to exculpate a behavior

the invocation of the absence of guilt is typically unlawful".

Accordingly, the plea is dismissed. ultimate responsibility

on the treatment continues to be attributed to the person in charge, who is the one who determines the

existence of the treatment and its purpose. Let us remember that, in general, the

operators process the data of their 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 (…). In this sense, ORANGE has

a network of sales representatives, points of sale and distributors approved through a

distribution contract to offer ORANGE services. Among these services

offered from their points of sale, is making duplicate SIM cards

corresponding to a mobile telephone line.

In the present case, it is proven that Orange provided a duplicate of the card

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

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

mobile, such as bank details, passwords, email address and others

personal data associated with the terminal. Thus, the defendant did not verify the

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

necessary for these events not to 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.

Well then, it is proven that Orange acknowledged in its response letter of

dated May 27 and in its allegations dated October 18, 2022 to this

Agency that the incident was due to a specific human error, by the Agent

of the Orange Point of Sale that, at the insistence and knowledge of the

delinquents from the company's 'slang' - so he thought he was dealing with a

partner- got the Agent to reveal his credentials, failing to comply

all the protocols and instructions communicated to him in connection with the

their confidentiality.

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

of the claimed party violates article 6.1 of the GDPR and may be 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."

IV.

Sanction

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 infraction;

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 circumstances:

-

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:

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

20/21

FIRST: IMPOSE ORANGE ESPAGNE, S.A.U., with NIF A82009812, 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 ORANGE ESPAGNE, 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 Law 39/2015, of October 1, on Administrative Procedure

Common of Public Administrations (hereinafter LPACAP), within the payment term

voluntary established in art. 68 of the General Collection Regulations, approved

by Royal Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003,

of December 17, by means of its income, indicating the NIF of the sanctioned and the number

of procedure that appears in the heading of this document, in the account

restricted IBAN number: ES00-0000-0000-0000-0000-0000, open in the name of the

Spanish Agency for Data Protection at the bank CAIXABANK, S.A..

Otherwise, it will proceed to its collection in the 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