 File No.: EXP202203638

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) dated March 1, 2022

filed a claim with the Spanish Data Protection Agency. The

claim is directed against ORANGE ESPAGNE, S.A.U. with NIF A82009812

(hereinafter, Orange) for the following reasons:

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

The complaining party states that, on February 24, 2022, it lost its line in

one of his two mobile phones. After contacting your telephone operator (entity

claimed) indicate that a duplicate of your SIM card had been made, request

that the claimant did not do, so he goes to a physical store and they provide him with the data

relating to said duplicate, the location being Barcelona, despite the fact that the claimant

resides in Madrid.

And, provide the following relevant documentation:

Copy of the claimant's ID.

Document related to the request for a duplicate SIM card. Point of Sale of

establishment of ***ESTABLISHMENT.1. There is no signature of the claimant.

Complaint filed with the Civil Guard of the town of Arganda del Rey

(Madrid), on February 25, 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 7, 2022 as

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

On May 9, 2022, this Agency received a written response

indicating: <<that on February 24 and 25 of this year, the duplicate was detected

of e-SIM usurping the identity of the claimant. The authors of the usurpation of

identity contacted an employee of the Point of Sale of the

establishment of ***ESTABLISHMENT.1 by accessing its login credentials

email accounts and other data to empty your bank accounts and/or Cryptocurrencies,

fact that has been denounced by this company at the end of March. This

extensive complaint of other previous cases, being prosecuted in case in which

preliminary proceedings 114/2022 of the Court of First Instance and Instruction no. 1 of

***LOCATION.1.

Well, once the credentials were obtained, it was when this person requested the

duplicate e-SIM exposed by the claimant. At the moment when the

claimant became aware of this circumstance and contacted this

mercantile, proceeding to block the line, as well as to make the adjustments

relevant.

In this regard, it should be noted that, in no case have they been affected or

the company's information security systems have been compromised, which

They have suffered a breach in their functioning.

Likewise, the access data to the systems of that point of sale have been updated,

so that they cannot be used again by the person who in bad faith carried out

out the irregular duplicate.

That they have implemented an action plan that is foreseen in the short term,

estimating to be able to launch it at the end (...) of 2022, materializing in the following

measures:

-

Implementation of a double identification factor.

- The project called “Whitelist IP”>>

THIRD: On May 17, 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 letter, and states: "That on February 24 and 25, 2022,

through Siebel 8 (internal Orange mobile card activation system

requested from stores), an order for a duplicate SIM (specifically an e-SIM)

associated with the Point of Sale of ***ESTABLISHMENT.1. the way it is

managed the e-SIM duplicate request, with the credentials of one of the

employees of the Point of Sale of ***ESTABLIECIÓN.1, but without monitoring

of the usual protocol (call to request authorization), causes the

Orange Fraud Department to identify and review the process in question.

The verification procedure for the application and granting of the e-SIM begins, with

in order to identify the existence of possible irregularities. While it was taking place

this verification process, the claimant gets in touch, on the same day, with

the Orange customer service department to report that he has been a victim of

impersonation, which serves to confirm suspicions about the

operation. Next, the Fraud department proceeds to categorize the

contracting as irregular and to cancel the duplicate e-SIM. Consequently,

Orange immediately makes the necessary adjustments. An alert is created indicating

that the client has been a victim of identity theft, and limiting the performance of

orders, to allow their control.

In the subsequent analysis of the factual assumption by the Analysis department
of Orange Risks, it was concluded that there had been a robbery of the
***ESTABLISHMENT.1 Point of Sale Siebel 8 credentials
(belonging to a third entity, franchisee of Orange). in the inquiries
it became known that, after deceiving one of the Point of Sale users,
he revealed his credentials, which were subsequently used to carry out
of the fraudulent procedure.
Consequently, it is concluded that the incidence is due to a specific human error,
by the Point of Sale Agent who, 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. These facts have been denounced by Orange,
stating the complaint with number of preliminary proceedings 114/2022 of the First Court
Instance and Instruction No. 1 of ***LOCATION.1. Likewise, in collaboration with the
authorities, Orange has proceeded to track the IMEI of the device from the
that the fraudulent eSIM duplicate was made, identifying it and including it
in an internal BlackList, so that it cannot be used again.
Likewise, the Claimant was informed from Orange of all the proceedings and
inquiries made. The Claimant continues to be an active customer of this
part.
On April 7, 2022, Orange receives the transfer of the claim filed by the
Claimant before the AEPD on the occasion of this factual assumption, responding
and attending to the issues that he presented through allegations that were
filed on May 9, 2022.
C / Jorge Juan, 6

In attention to the present assumption of fact that concerns us, I would like this part to review that, although until now the identity of Orange customers was impersonated, now the identity of Orange employees and agents is impersonated.

Mobile applications are installed on the specific mobile device, so for be able to access them, identity theft should have or with additional information from the Claimant, or with their mobile terminal. In this sense, the Agency is not capable of justifying that it actually had knowledge of this information by criminals during the process of duplicate. Therefore, beyond the theoretical conceptualization of the data included on a SIM card as personal data, it has not been proven that your confidentiality has been compromised.

In the present case, the existence of a strict control, prior and post-hiring, the establishment of prior and subsequent measures, as well as such as the existence of specific measures aimed at avoiding the commission of these practices (already indicated by this part in the allegations to the requirement of information from the AEPD). That is why it is not possible to assess the guilt of Orange in the present supposition of fact, not being legally valid the assessment made by the Agency for commission of infringement by this company.

"In this case, once the reasons given by ORANGE ESPAGNE have been analysed, 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. of the

Otherwise, we would find ourselves in a situation of defenselessness and legal uncertainty

for Orange.

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 indicates the file of Procedure No.: PS/03638/2022.

Alternatively, in the event that the AEPD decides against the

legal basis 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 contained in the Commencement Agreement notified to Orange”

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 10, 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 2 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:

"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 this sense, the AEPD ignores the fact that ORANGE has developed and implemented a protocol for requesting a duplicate of the SIM card, and communicated to the agents in charge of processing these requests. Not the slightest consideration is included about its content or the adequacy of the itself to assess the display of diligence that ORANGE has undertaken.

The fact that the protocol has not been followed constitutes a breach contractual by the agent of the collaborating entity, sanctioned by ORANGE (who does not have the legal capacity to act directly against the agent, so directed against your employer). In this sense, it is inappropriate purported personification of ORANGE, as if the entity materially executed some action.

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 indicates the file of Procedure No.: PS/03638/2022. Secondarily, in

the case that the AEPD resolves against the legal grounds that sustain

Orange, the AEPD is requested to take into account the extenuating circumstances

based on the previous allegations and, consequently, conclude the

procedure by means of a warning and, ultimately, if you consider that

the imposition of a sanction proceeds, moderates or modulates its proposal included in the

Sanction proposal notified to Orange, based on the arguments expressed

in the body of this brief of allegations".

In view of all the proceedings, by the Spanish Agency for Data Protection

In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: The claimant states that, on February 24, 2022, he ran out of

line on one of his two mobile phones. After contacting Orange, they tell him that

a duplicate of his SIM card had been made, a request that the claimant did not make,

so you go to a physical store and they provide you with the data related to said duplicate,

the locality being Barcelona, despite the fact that the claimant resides in Madrid.

SECOND: The claimant has provided a copy of the complaint filed

before the Civil Guard of the town of Arganda del Rey (Madrid) for these facts and

document relating to the request for a duplicate SIM card. Point of Sale of

establishment of *** ESTABLISHMENT.1, not containing the signature of the claimant.

THIRD: Orange states that on February 24 and 25, 2022 the

through Siebel 8 (internal Orange mobile card activation system

requested from stores), an order for a duplicate SIM (specifically an e-SIM)

associated with the Point of Sale of ***ESTABLISHMENT.1. The fraud department

proceeds to categorize the contract as irregular and to cancel the duplicate e-SIM.

FOURTH: Orange acknowledged in the response brief dated October 18,

2022 to this Agency that the incident is due to a specific human error, by

of the Orange Point of Sale Agent who, at the insistence and knowledge of

the criminals of the company's 'slang' - so he believed he was dealing with

a colleague - got the Agent to reveal his credentials, in breach of

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

their confidentiality.

FIFTH: These facts have been denounced by Orange, stating the complaint with

No. of preliminary proceedings 114/2022 of the Court of First Instance and Instruction No. 1

of ***LOCATION.1. Likewise, in collaboration with the authorities, from Orange

the IMEI of the device from which the duplicate was made has been traced

of fraudulent eSIM, identifying it and including it in an internal BlackList,

so that it cannot be used again.

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 this sense, it should be clarified that the card is inserted inside the mobile terminal.

SIM. It is a smart card, made of plastic and small dimensions, which contains a

chip in which the service key of the subscriber or subscriber used to

identify yourself to the network, that is, the customer's mobile phone number

MSISDN (Mobile Station Integrated Services Digital Network -Mobile Station Network

Digital de Servicios Integrados-), as well as the personal identification number of the

IMSI (International Mobile Subscriber Identity) subscriber

Mobile subscriber-) but can also provide other types of data such as information

tion on the telephone list or the calls and messages list.

The SIM card can be inserted in more than one mobile terminal, as long as it is

be released or from the same company.

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:

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.

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.

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.

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.

Orange recognized in its allegations dated October 18 and December 12,

2022 to this Agency that the incident is due to a specific human error, by

of the Orange Point of Sale Agent who, at the insistence and knowledge of

the criminals of the company's 'slang' - so he believed he was dealing with

a colleague - got the Agent to reveal his credentials, in breach of

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, in an initial assessment,

The following factors are considered concurrent in this case:

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:

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

938-181022

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es