

□ File No.: EXP202202151

RESOLUTION OF TERMINATION OF THE PROCEDURE FOR PAYMENT

VOLUNTEER

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

BACKGROUND

FIRST: On March 17, 2023, the Director of the Spanish Agency for
Data Protection agreed to start a sanctioning procedure against ORANGE ESPAGNE,
S.A.U. (hereinafter, the claimed party), through the transcribed Agreement:

<<

File No.: EXP202202151

AGREEMENT TO START THE SANCTION PROCEDURE

Of the actions carried out by the Spanish Data Protection Agency and in
based on the following:

FACTS

FIRST: D.A.A.A. (hereinafter, the claiming party) dated January 12,
2022 filed a claim with the Spanish Data Protection Agency. The
claim is directed against ORANGE ESPAGNE, S.A.U. with NIF A82009812 (in
below, the claimed party or ORANGE). The reasons on which the claim is based
are the following:

The claimant states that on December 2, 2021, he received a message
of ORANGE in which he was informed that the service of diversion of
calls, which I had not requested.

The claimed party authorized without their consent a diversion of data from their mobile
to a third line that is not owned and unknown.

In addition, they had accessed their bank accounts, making various charges and unauthorized operations.

Relevant documentation provided by the claimant:

- Screenshots of WhatsApp conversation mobile terminal of date

12/02/2021 with ORANGE where it is manifested, by ORANGE:

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

2/14

1. That the claimant on December 2, 2021 contacted ORANGE, per call, several times to order the activation and deactivation of the call forwarding service to another number since the card was damaged.

2. That the query line was ***TELEPHONE.1.

3. That the first interaction on 12/02/2021 was at 5:16:53 p.m. and was carried out by means of call.

4. That they cannot show which line they called from, but it is indicated on the note that it was from the claimant's line.

- Copy of police report dated 12/03/2021 where the following manifestations:

1. That the events occurred on 12/02/2021.

2. That, according to the claimant, there were irregular charges not authorized by him made on various bank cards that appear in his name and that are associated with your bank account number ES00 0000 0000 0000 0000.

3. That prior to this, the claimant's mobile phone showed a wrong operation from 5:16 p.m. to 7:14 p.m. on that day 12/02/2021, no

being able to make or receive calls. That third parties could call you to your line by contacting the phone number ***TELEPHONE.2 (forwarding call). That this number does not correspond to that of the claimant.

4. That, after the time interval described, recovers complete control from your telephone terminal, being able to operate again with it.

5. That the claimant has presumably been the victim of a SIM scam SWAPPING (second generation).

6. The statement that the claimant provides various documentation and bank statement that supports the above.

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 February 22, 2022 as It appears in the acknowledgment of receipt that is in the file.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/14

On March 22, 2023, this Agency received a written response

indicating: "In relation to the foregoing, and in terms of call forwarding, indicate to

this Agency that on December 2 a call is received from an individual, claiming to be the owner of the line, and providing the operator with the identifying data necessary to confirm your identity as the owner of the line.

In this way, it pretends to be the claimant, overcoming security measures.

commercial security, which consist, among others, of accrediting knowledge of very specific data of the owner that it is difficult for any other person to know,

After that, he requests, alleging that his SIM card had suffered damage and was not 100% operational, a forwarding of calls from the claimant's number to a different mobile numbering, claiming to be having problems, among others, for the SMS reception.

In his communications with this company on the occasion of the incident, the claimant indicated that the authorization of the diversion had allowed the criminal who had become go through it access the applications of your bank and the SMS of verification sent by it, so that it had been able, ultimately,

access the content of their accounts and subtract certain amounts of money. TO

In this regard, it should be noted that, as indicated to the claimant, the deviations of

Calls do not entail, in any case, access to the mobile applications of the number of origin, to your data or to your SMS messages, since the only thing that is diverts is the incoming call traffic as such, not being possible to access

no other type of information of the original number, so the operations

bank transactions that could be carried out at that time must have been verified by methods other than those described above. In short, from the

new number cannot access the data, applications or messages of the number

old, in short, to any type of information other than incoming calls.

In this sense, it has been possible to verify, after a study derived from the reception of the present claim, made in order to clarify what happened, that the staff of

customer service of the company, after receiving customer communications, and as reflects the documentation attached to the request, proceeded immediately, to cancel call forwarding. In addition, the risk analysis group was transferred of the company to carry out a study of the situation, determining that the request for call forwarding had been irregular and that it had occurred by another person, notwithstanding that the caller, exceeding the measures of previously described security, will be satisfactorily identified as the individual which he now claims.

Derived from the above, said group was able to verify that, even prior to his analysis, the Customer Service staff had already rolled back the diversion, and, in addition, they disabled any future requests regarding the itself, so that this type of procedure can only be carried out by the holder of the line either in a physical store or by calling from the numbering object of the contract, including a notice about it in the company's computer systems so that said instruction is made clear to all of its employees that access the claimant's file, all this, taking into account that there is a third party in bad faith who, knowing your data, is using it to carry out transactions on your behalf.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

4/14

Measures adopted so that similar incidents do not occur After the analysis referred to in the previous section, the risk analysis group has proceeded, and with the In order to avoid this situation in the future, to communicate the case and the use that is being

making the caller numbering, to the competent authorities, so that the

They can carry out the investigations and investigations that they consider timely.

In addition, and internally, said numbering is also included in the blacklist of the company, so that requests for said telephone number are not answered in relation to this and other types of procedures”.

THIRD: On April 4, 2022, in accordance with article 65 of the LOPDGDD, the claim presented by the claimant party was admitted for processing.

FOURTH: The General Subdirectorate of Data Inspection proceeded to carry out of previous investigative actions to clarify the facts in

matter, by virtue of the functions assigned to the control authorities in the article 57.1 and the powers granted in article 58.1 of the Regulation (EU)

2016/679 (General Data Protection Regulation, hereinafter GDPR), and

in accordance with the provisions of Title VII, Chapter I, Second Section, of the LOPDGDD, having knowledge of the following extremes:

RESULT OF INVESTIGATION ACTIONS

As a consequence of the request for information, on November 10, 2022, ORANGE sends this Agency the following information and statements:

- 1.
- 2.
- 3.

That there is no request for a duplicate SIM card but that the events that occurred related to a call forwarding request.

That when calls are diverted from one telephone line to another it does not imply a forwarding of SMS messages. That call forwarding and forwarding of messages are two separate performances each subjected to

verification procedures. That, so if fraud occurs, the holder of the line continues to have access to text messages, so you will receive Notifications of possible fraudulent uses carried out by the identity theft, for example, when carrying out a banking or buys.

Manifest:

“[...]

As indicated in the Allegations dated March 22, 2022, the Claimant received a communication via SMS indicating that you had activated a call forwarding from your phone number to another line different phone number After being informed of these facts, Orange proceeded to evaluate what happened by the corresponding internal departments, and was able to verify that on December 2, 2021 a call is received from a individual, claiming to be the owner of the line, and providing the operator with the

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

5/14

identifying data of the same, as well as all the necessary to confirm your identity as owner of the line.

In this way, the impersonator posed as the Claimant, overcoming the security measures established by Orange for their identification, by accredit knowledge of very specific data that should only be known by the headline. After that, he requests, alleging that his SIM card had suffered malfunctioned and was not working properly, a call forwarding

from the telephone number contracted with Orange to a mobile numbering different.

That is to say, that the identity theft had in his possession the data personal information of the Claimant prior to the claimant having contact any with Orange, and it was with these data that he managed to overcome the issues for their identification, which shows that the delinquent does not He accessed them through this merchant.

After being transferred to the Risk Analysis Group, it concluded that the Claimant had probably been a victim of phishing, smishing or some another tool of social engineering.

In this sense, it should be noted that, despite the fact that Orange establishes measures and submit them to review and continuous improvement, it is essential that individuals, as holders of their personal data, have certain diligence when it comes to custody, without making them available to third parties or neglecting your credentials, allowing third parties to get hold of your information personal, so that they facilitate their impersonation.

[...]"

That among the ways available to customers to request a diversion of call is found via telephone through the Customer Service Customer.

In general, for a customer to request a call forwarding must overcome the Security Policy.

That the Security Policy through the telephone via Attention to the Client, until 09/28/2022, consisted of the Mobile Connect tool which is the identity validation tool in the Customer Service system Client for call forwarding requests.

Provides recording of the call by the impersonator to ORANGE that made the request for call forwarding where it is stated that the information requested from the client is exclusively name and surname, ID number, date of birth, address and zip code.

4.

5.

6.

7.

CONCLUSIONS:

1.

ORANGE acknowledges that there was an identity theft in the activation of the call forwarding of the claimant's line.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

6/14

2.

As stated in the recording of the call and in the security policy contributed:

The security policy does not state the types of questions that are can do to authenticate a client, although it is clear that they must ask yourself 3 questions for this purpose. Apart from the name and surname and number DNI, which are data to identify the client, not to authenticate it, it is only they asked 2 more questions; "date of birth" and "address" (in the latter must be understood including that of the "postal code").

In addition, ORANGE states that the data that is asked to verify the identity vary between personal economic, identification and customer contact, such as: ID digits, phone line digits telephone numbers, amount of invoices collected, contract number, digits of the associated bank account. However, the data that is actually asked were exclusively name and surname, ID number, date of birth, address and zip code.

3.

It has not been possible to verify that a call forwarding also produces a forwarding of SMS messages.

FIFTH: According to the report collected from the AXESOR tool, the entity ORANGE ESPAGNE, S.A.U. is a large company established in 1998, and with a turnover of 4,272,121,000 euros in the year 2021.

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

Breached Obligation

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

www.aepd.es

C / Jorge Juan, 6

28001 – Madrid

sedeagpd.gob.es

7/14

Article 6 of the GDPR, "Legacy of the treatment", which indicates in its section 1 the cases in which the processing of third-party data is considered lawful:

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

conditions:

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

for one or more specific purposes;

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

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

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

responsible for the treatment;

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

Physical person;

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

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

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

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

interests do not outweigh the interests or fundamental rights and freedoms of the interested party that require the protection of personal data, in particular when the interested is a child. The provisions of letter f) of the first paragraph shall not apply. application to processing carried out by public authorities in the exercise of their functions”.

II

Classification and classification of the offense

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 LOPDGD, for the purposes of the prescription of the infringement, qualifies in its article 72.1 very serious infringement, in this case the limitation period is three years, "b)

The processing of personal data without the fulfillment of any of the conditions of legality of the treatment established in article 6 of Regulation (EU) 2016/679”.

In the present case, it is proven that a third party requested a change of services to the claimed party, that is, the activation of call forwarding due to fracture, supposedly, from the SIM card.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Well then, in its response dated December 22, 2022, the defendant recognizes that there was an identity theft in the activation of the diversion of claimant hotline call.

However, as stated in the recording of the call and in the security policy provided, three questions should be asked. Apart from the name and surname and number of the DNI, which are data to identify the client, not to authenticate it, it is only They asked two more questions; date of birth" and "address" (in the latter you must understood to include the "zip code").

In addition, ORANGE states that the data that is asked to verify the identity vary between economic, identification and contact personal data of the client, such as: ID digits, telephone line digits, amount of invoices collected, contract number, digits of the associated bank account. Without However, the data that was actually asked was exclusively name and surnames, ID number, date of birth, address and postal code.

Based on the foregoing, in the case analyzed, the diligence used by the defendant to identify the person who requested call forwarding.

In any case, the procedure implemented by the claimed party was not followed, since, if it did, the diversion activation should have been denied of calls.

In view of the foregoing, the claimed party fails to prove that this procedure and therefore there was an illegal treatment of the personal data of the complaining party, thereby contravening article 6 of the GDPR.

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 proposal

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

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

9/14

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 person in charge or in charge of the treatment to

settle the damages suffered by the interested parties;

d) the degree of responsibility of the person in charge or of the person in charge of the treatment, habi-

gives an account of the technical or organizational measures that have been applied by virtue of the

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 certification mechanisms.

fications approved in accordance with article 42, and

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

as the financial benefits obtained or the losses avoided, directly or indirectly.

mind, through infraction.”

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

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.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

10/14

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 transcribed precepts, and without prejudice to what results from the instruction of the procedure, in order to set the amount of the fine to impose on the entity claimed as responsible for an infringement classified in the 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:

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

The claimed party proceeded to resolve the incident that is the subject of the claim

effective (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 foregoing, by the Director of the Agency

Spanish Data Protection.

HE REMEMBERS:

FIRST: INITIATE SANCTION PROCEDURE against ORANGE ESPAGNE,

S.A.U. with NIF A82009812, for the alleged violation of article 6.1) typified in the

Article 83.5.a) of the aforementioned GDPR.

SECOND: APPOINT as instructor D. B.B.B. and as secretary to Ms. C.C.C.,

indicating that any of them may be challenged, if applicable, in accordance with the provisions

established in articles 23 and 24 of Law 40/2015, of October 1, on the Legal Regime

co of the Public Sector (LRJSP).

THIRD: INCORPORATE into the disciplinary file, for evidentiary purposes, the

claim filed by the claimant and its documentation, the documents

obtained and generated by the General Subdirectorate of Data Inspection.

FOURTH: THAT for the purposes provided for in art. 64.2 b) of Law 39/2015, of 1

October, of the Common Administrative Procedure of Public Administrations, the

sanction that could correspond would be for the infringement of article 6.1 of the GDPR,

typified in article 83.5 a) of the GDPR, the sanction that would correspond would be a

fine for an amount of 70,000 euros (seventy thousand euros) without prejudice to what is

of the instruction.

FIFTH: NOTIFY this agreement to ORANGE ESPAGNE, S.A.U. with NIF

A82009812 granting a hearing period of ten business days to formulate

the allegations and present the evidence it deems appropriate. In his writing of allegations must provide your NIF and the procedure number that appears in the heading of this document.

If, within the stipulated period, he does not make allegations to this initial agreement, the same may be considered a resolution proposal, as established in article 64.2.f) of Law 39/2015, of October 1, on the Common Administrative Procedure of Public Administrations (hereinafter, LPACAP).

In accordance with the provisions of article 85 of the LPACAP, in the event that the sanction to be imposed other than a fine, may recognize its responsibility within the term granted for the formulation of allegations to the present initiation agreement; it which will entail a reduction of 20% for the sanction that should be imposed in this proceeding, equivalent in this case to fourteen thousand euros (€14,000).

With the application of this reduction, the amount of the sanction would be established in fifty-six thousand euros (€56,000), resolving the procedure with the imposition of this sanction.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

12/14

In the same way, it may, at any time prior to the resolution of this procedure, carry out the voluntary payment of the proposed sanction, in accordance with the provisions of article 85.2 LPACAP, which will mean a reduction of 20% of the amount of the same, equivalent in this case to fourteen thousand euros (€14,000), for the alleged offence. With the application of this reduction, the amount of the sanction would be established at fifty-six thousand euros (€56,000) and

Your payment will imply the termination of the procedure, without prejudice to the imposition of the corresponding measures.

The reduction for the voluntary payment of the penalty is cumulative to the corresponding apply for acknowledgment of responsibility, provided that this acknowledgment

of the responsibility is revealed within the period granted to formulate

allegations at the opening of the procedure. Voluntary payment of the referred amount

in the previous paragraph may be done at any time prior to the resolution. In

In this case, if both reductions were to be applied, the amount of the penalty would remain established at forty-two thousand euros (€42,000).

In any case, the effectiveness of any of the two aforementioned reductions will be

conditioned to the withdrawal or resignation of any action or appeal via

administrative against the sanction.

In the event that you choose to proceed with the voluntary payment of any of the amounts

previously indicated, 56,000 euros or 42,000 euros, you must make it effective

by depositing it in the account number ES00 0000 0000 0000 0000 0000 opened to

name of the Spanish Data Protection Agency at CAIXABANK Bank,

S.A., indicating in the concept the reference number of the procedure that appears in

the heading of this document and the reason for reducing the amount to which

welcomes.

Likewise, you must send proof of income to the General Subdirectorate of

Inspection to continue with the procedure in accordance with the quantity

entered.

The procedure will have a maximum duration of nine months from the

date of the initiation agreement or, where appropriate, of the draft initiation agreement.

After this period, its expiration will occur and, consequently, the file of

performances; in accordance with the provisions of article 64 of the LOPDGDD.

Finally, it is noted that in accordance with the provisions of article 112.1 of the LPACAP, there is no administrative appeal against this act.

Mar Spain Marti

Director of the Spanish Data Protection Agency

>>

SECOND: On April 24, 2023, the claimed party has proceeded to pay the sanction in the amount of 42,000 euros making use of the two reductions provided for in the initiation Agreement transcribed above, which implies the recognition of responsibility.

THIRD: The payment made, within the period granted to formulate allegations to the opening of the procedure, entails the waiver of any action or appeal via www.aepd.es

C / Jorge Juan, 6

28001 – Madrid

sedeagpd.gob.es

13/14

against the sanction and acknowledgment of responsibility in relation to the facts referred to in the Commencement Agreement.

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: "The 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

Termination of the procedure

Article 85 of Law 39/2015, of October 1, on Administrative Procedure

Common for Public Administrations (hereinafter, LPACAP), under the heading

"Termination in disciplinary proceedings" provides the following:

"1. Initiated a disciplinary procedure, if the offender acknowledges his responsibility,

The procedure may be resolved with the imposition of the appropriate sanction.

2. When the sanction has only a pecuniary nature or it is possible to impose a

pecuniary sanction and another of a non-pecuniary nature but the

inadmissibility of the second, the voluntary payment by the presumed perpetrator, in

any moment prior to the resolution, will imply the termination of the procedure,

except in relation to the replacement of the altered situation or the determination of the

compensation for damages caused by the commission of the offence.

3. In both cases, when the sanction is solely pecuniary in nature, the

The competent body to resolve the procedure will apply reductions of at least

20% of the amount of the proposed penalty, these being cumulative among themselves.

The aforementioned reductions must be determined in the notification of initiation

of the procedure and its effectiveness will be conditioned to the withdrawal or resignation of

any administrative action or resource against the sanction.

The percentage reduction provided for in this section may be increased

according to regulations."

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

14/14

According to what has been stated,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: DECLARE the termination of procedure EXP202202151, in

in accordance with the provisions of article 85 of the LPACAP.

SECOND: NOTIFY this resolution to ORANGE ESPAGNE, S.A.U..

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 as prescribed by

the art. 114.1.c) of Law 39/2015, of October 1, on Administrative Procedure

Common of Public Administrations, interested parties may file an appeal

administrative litigation before the Administrative Litigation 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.

Mar Spain Marti

Director of the Spanish Data Protection Agency

936-040822

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es