

□ File No.: PS/00611/2021

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 February 3, 2022, the Director of the Spanish Agency for
Data Protection agreed to initiate a sanctioning procedure against VODAFONE
SPAIN, S.A.U. (hereinafter the claimed party). Notified the agreement of initiation and
After analyzing the allegations presented, on April 1, 2022, the
proposed resolution that is transcribed below:

<<

File number: PS/00611/2021

PROPOSED RESOLUTION OF PUNISHMENT PROCEDURE

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

BACKGROUND

FIRST: Dated 11/14/2020, it is registered with the Spanish Protection Agency
of Data a document from the claimant stating that:

“A person called Vodafone on 10/27/2020 by telephone and posing as
for him, he bought an Iphone 12 and changed the rates he had contracted. signed a
contract in your name by changing your phone number (**PHONE.1), your email
(**EMAIL.1) and your date of birth (**DATE.1). The contract for the purchase of
terminal included an initial payment of 49 euros, 24 monthly installments of 38.01 euros and a
final payment of 96 euros, all debited to my checking account. Received an SMS from

Vodafone with a link to the new contract that he did not read until 10/29/2020 He attended to the offices of the Civil Guard in ***LOCALIDAD.1 (Valladolid) to file the relevant complaint. He called Vodafone and they agreed to send him in a few hours the recordings of the calls and the signing of the contract made in a telephone. But they didn't. He called again and was told that they would be sent to him in a few days. Neither did they. He called again and was told that there were no recordings, that it was done with an electronic signature and they would call it a fraud. But they didn't call him either. He called again and was told that there was no fraud and that they had reversed some changes but the contract is still there, the debt and the permanence".

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

2/20

Attach to your claim, among others, the following documents:

- Copy of the contract between VODAFONE and the claimant dated October 27

of 2020 where your contact address, name, surnames and DNI and

as contact telephone number the number ***PHONE.1 and in the email field

***EMAIL.1 appears and where it also appears in the section "Data of

devices" an Iphone 12 with mobile line number ***PHONE.2.

- Copy of the complaint filed with the Civil Guard.

SECOND: In view of the facts set forth in the claim and the documents

provided with it, the General Subdirectorate of Data Inspection proceeded to carry out

preliminary investigative actions to clarify the facts,

in accordance with the provisions of Title VII, Chapter I, Second Section, of the Law

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

digital rights (hereinafter LOPDGDD).

The Data Inspection of the AEPD addressed a request to the accused informative, requesting that:

Within a maximum period of one month, from the receipt of this letter, you must analyze the claim and send this Agency the following information:

1. The decision made regarding this claim.
2. In the event of exercising the rights regulated in articles 15 to 22 of the RGPD, accreditation of the response provided to the claimant.
3. Report on the causes that have motivated the incidence that has originated the claim.
4. Report on the measures adopted to prevent the occurrence of similar incidents, dates of implementation and controls carried out to verify its effectiveness.
5. Any other that you consider relevant.

The notification of the aforementioned requirement, according to documentation that works in the file was accepted on 12/16/2020.

The respondent did not reply within the period granted for this purpose.

THIRD: On 03/29/2021 VODAFONE ESPAÑA, S.A. refer to this Agency the following information and statements:

1. That the contract was classified as fraudulent on 11/05/2020, having issued the corresponding installments.
2. That the claimant is currently registered as a customer in his systems.
3. That on 10/27/2020 they registered the acceptance of an offer through of the Teleshopping channel through which a mobile was acquired and some of the personal data associated with the claimant's account, specifically, date of

birth, email address and contact telephone number.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/20

4. That the fraudulent acquisition of a mobile terminal was made by providing the

personal data of the claimant, acting in accordance with the Privacy Policy

Security for contracting by private clients. That is, they required

to the contracting party name and surnames as well as the DNI.

5. That based on a call from the claimant's wife dated

10/29/2020 is when they became aware of what happened.

6. That in no way could they know at the time of hiring

that the one who made the phone call in which the fraudulent order was made, did not

was the claimant, since he provided all his data correctly: name, surnames and

DNI.

7. That the claimant was a VODAFONE customer.

Provide a copy of the letter sent to the claimant dated 03/23/2021.

It provides a screenshot of its systems where there is a call from the

line ***PHONE.1 accepting the offer associated with the claimant.

Provides screenshots of their systems where there is a call from the

claimant requesting the recording of 10/27/2020 and where the "historical" field is

partially displayed, VODAFONE stating that at the end of said field there is

"We verified that there is no recording of the indicated date 10/27/20"

It provides a screenshot of its systems where the caller appears as the

claimant, "date of creation" states "11/03/2020" and "opening code" states

“Data impersonation”.

It provides a screenshot of its systems associated with the claimant where appears in the "Service Information" field and within it, in the "Package contracted" states “There is no package. WITHOUT ACTIVE MOBILE”.

FOURTH: On 03/31/2021 the claimant sends this Agency the following information and manifestations:

1. That you need to access the recording.
2. That the contract was made from another telephone number that was not headline.

Provides VODAFONE invoice with billing period from 01/22/2021 to 02/21/2021 where there are payment fees related to a mobile terminal associated with the line ***PHONE.2.

FIFTH: Dated 08/12/2021 VODAFONE ESPAÑA, S.A. sends to this Agency the following information and statements:

1. Provide screenshots of your systems already provided previously and where now it is stated in added text "I confirm that the offer is accepted by

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

4/20

call made from the line ***PHONE.1, which is in the name of another client

A.A.A. ***NIF.1”

2. Provides a screenshot of the Security Policy where it is stated that will request “HOLDER: Customer service access code or DNI. NOT HOLDER: Customer service access key.

3. That the recording is not available.

4. Provide a copy of the contract without signature by the claimant. the claimed states that "[...] a copy of the contract that is automatically generated by the system once the recording is made to the interested party for the contracting of the services of Vodafone. In relation to the latter, [...], it is not available in the Vodafone systems, so it cannot be provided in this proceeding."

SIXTH: On February 3, 2022, the Director of the Spanish Agency for Data Protection agreed to initiate a sanctioning procedure 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 the Public Administrations (in hereinafter, LPACAP), for the alleged violation of Article 6.1 of the RGPD, typified in Article 83.5 of the RGPD.

SEVENTH Having notified the aforementioned initiation agreement on 02/07/2022, the party claimed He presented on 02/21/2022 a brief of allegations in which, after referring to his integrity to what he calls the "arguments presented" on March 23, 2021 (hereinafter, the "Arguments Brief of March 23") and August 12, 2021 (hereinafter, the "August 12 Arguments Brief"), in summary, stated that:

1) Acted in accordance with the Security Policy for hiring by private clients. The First Allegation is devoted to this question.

2) Subsidiarily, in the event that the Agency understands that Vodafone has infringed article 6.1 of the RGPD, the existence of guilt cannot be assessed in the infringement imputed to Vodafone and, consequently, cannot be imposed on the same penalty. The Second Argument is devoted to this question.

3) Subsidiarily to points 1) and 2) above, and in the event that the Agency understands that there has been an infraction and a sanction must be imposed on Vodafone,

the mitigating circumstances identified in the Allegation must be taken into account

Third.

Based on the exposed arguments, it requests that having presented this document and all the documents that accompany it and, by virtue of it, consider that the statements contained therein and, after the appropriate procedures, agree:

1) The dismissal of the file with the consequent filing of the proceedings, for not having committed any of the imputed infractions.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

5/20

2) Subsidiarily, that if any sanction is imposed, it is imposed in the amount minimum, in light of the extenuating circumstances indicated in this document.

EIGHTH: Attached as an annex is a list of documents in the process.

Of the actions carried out in this procedure and the documentation in the file, the following have been accredited:

PROVEN FACTS

FIRST: Dated 11/14/2020, it is registered with the Spanish Protection Agency of Data a document from the complaining party stating that:

“A person called Vodafone on 10/27/2020 by telephone and posing as for him, he bought an Iphone 12 and changed the rates he had contracted. signed a contract in your name by changing your phone number (**PHONE.1), your email (**EMAIL.1) and your date of birth (**DATE.1). The contract for the purchase of terminal included an initial payment of 49 euros, 24 monthly installments of 38.01 euros and a

final payment of 96 euros, all debited to my checking account. Received an SMS from Vodafone with a link to the new contract that he did not read until 10/29/2020 He attended to the offices of the Civil Guard in ***LOCALIDAD.1 (Valladolid) to file the relevant complaint. He called Vodafone and they agreed to send him in a few hours the recordings of the calls and the signing of the contract made in a telephone. But they didn't. He called again and was told that they would be sent to him in a few days. Neither did they. He called again and was told that there were no recordings, that it was done with an electronic signature and they would call it a fraud. But they didn't call him either. He called again and was told that there was no fraud and that they had reversed some changes but the contract is still there, the debt and the permanence”.

Attach to your claim, among others, the following documents:

- Copy of the contract between VODAFONE and the claimant dated October 27 of 2020 where your contact address, name, surnames and DNI and as contact telephone number the number ***PHONE.1 and in the email field ***EMAIL.1 appears and where it also appears in the section "Data of devices" an Iphone 12 with mobile line number ***PHONE.2.
- Copy of the complaint filed with the Civil Guard.

SECOND: VDF acknowledges in its letter of 03/29/2021:

1. That the contract was classified as fraudulent on 11/05/2020, having issued the corresponding installments.
2. That the claimant is currently registered as a customer in his systems.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3. That on 10/27/2020 they registered the acceptance of an offer through of the Teleshopping channel through which a mobile was acquired and some of the personal data associated with the claimant's account, specifically, date of birth, email address and contact telephone number.

4. That the fraudulent acquisition of a mobile terminal was made by providing the personal data of the claimant, acting in accordance with the Privacy Policy Security for contracting by private clients. That is, they required to the contracting party name and surnames as well as the DNI.

5. That based on a call from the claimant's wife dated 10/29/2020 is when they became aware of what happened.

6. That the claimant was a VODAFONE customer.

7. According to a screenshot of their systems, there is a call from the line ***PHONE.1 accepting the offer associated with the claimant.

THIRD: VDF acknowledges in its letter of 08/12/2021:

1. What is recorded in their information systems in relation to the call made on 10/27/2020 for the contracting of services "that the offer is accepted for a call made from the ***TELEPHONE.1 line, which is in the name of another client A.A.A. ***NIF.1"

2. That its Security Policy states that "HOLDER: Password customer service access or DNI. NON-HOLDER: Customer service access code client".

3. That their information systems state "that the recording of the interested party for contracting Vodafone services is not available in the Vodafone systems, so it cannot be provided in this procedure"

FOUNDATIONS OF LAW

Yo

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

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

control authority and as established in articles 47 and 48.1 of the Law

Organic 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 Data Protection Agency.

Likewise, article 63.2 of the LOPDGDD determines that: "The procedures

processed by the Spanish Agency for Data Protection will be governed by the provisions

in Regulation (EU) 2016/679, in this organic law, by the provisions

regulations issued in its development and, as long as they do not contradict them, with a

subsidiary, by the general rules on administrative procedures."

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

7/20

II

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

the next:

Before entering to answer the content of the allegations, it is necessary to

some clarifications in relation to the dates regarding what in his writing of

allegations VDF calls "The infraction is caused by the following facts":

In the first place, there is an error regarding the dates of the call of the alleged

offender, the contracting of the acquisition of a mobile device, the change of rates

contracted and the modification of data; as well as the sending of the SMS to the telephone of the

claimant, the filing of his complaint with the Civil Guard and his communication to VDF of the possible fraudulent action of the presumed fraudster; Y also of the date in which the facts are classified as fraud. VDF indicates in its brief of allegations as the year in which they take place the year 2021 when actually occur in the year 2020.

Secondly, the AEPD makes available to VDF the electronic notification of the transfer of the claim of the complaining party on 12/15/2020, not on 12/16/2020, which is the day on which VDF accesses the electronic notification and is understood notified for administrative purposes, in accordance with the provisions of article 43 of the Law 39/2015, of October 1, on the Common Administrative Procedure of the Public Administrations (hereinafter LPAC), which provides that:

"1. Notifications by electronic means will be made by appearance at the electronic headquarters of the Administration or Acting Body, through the single enabled electronic address or through both systems, as available each Administration or Organism.

For the purposes provided in this article, it is understood by appearance at the headquarters electronically, access by the interested party or his duly identified representative to the notification content.

2. Notifications by electronic means shall be understood to have been made in the moment in which access to its content occurs.

When notification by electronic means is mandatory, or has been expressly chosen by the interested party, it will be understood as rejected when they have Ten calendar days have elapsed since the notification was made available without access to its content.

3. The obligation referred to in article 40.4 shall be deemed fulfilled with the made available for notification in the electronic headquarters of the Administration or

Acting body or at the unique authorized electronic address.

4. The interested parties will be able to access the notifications from the Access Point

Electronic General of the Administration, which will function as an access portal”.

Thirdly, although VDF's reply brief to the transfer of the file

figure signed on 03/23/2021 the answer is not understood to be made until

the brief is filed in the registry, that is, on 03/29/2021. Although, although both in one

date as another the answer is produced outside the term established for that purpose for

carry it out, the statements of VDF contained in said document were taken into account.

written at the time of dictating the initiation agreement.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

8/20

Fourth, the AEPD makes available to VDF the electronic notification of the

request for information on 07/28/2021, not on 08/02/2021, which is the day on which

VDF agrees to the electronic notification and is understood to have been notified for

administrative, in accordance with article 43 of the LPAC.

Entering to analyze the content of his pleadings brief, as already indicated in the

seventh precedent of this proposal, after referring in its entirety to what

refers to the "arguments presented" on March 23, 2021 (hereinafter,

the “Brief of Arguments of March 23”) and August 12, 2021 (hereinafter, the

"Brief of Arguments of August 12"), in relation to the requirements of

information E/10012/2020 and E/02109/2021; VDF articulates its defense based on the

following allegations:

1) Acted in accordance with the Security Policy for hiring by

private clients. The First Allegation is devoted to this issue.

2) Subsidiarily, in the event that the Agency understands that Vodafone has infringed article 6.1 of the RGPD, the existence of guilt cannot be assessed in the infringement imputed to Vodafone and, consequently, cannot be imposed on the same penalty. The Second Argument is devoted to this issue.

3) Subsidiarily to points 1) and 2) above, and in the event that the Agency understands that there has been an infraction and a sanction must be imposed on Vodafone, the mitigating circumstances identified in the Allegation must be taken into account Third.

Based on the exposed arguments, it requests that having presented this document and all the documents that accompany it and, by virtue of it, consider that the statements contained therein and, after the appropriate procedures, agree:

- 1) The dismissal of the file with the consequent filing of the proceedings, for not having committed any of the imputed infractions.
- 2) Subsidiarily, that if any sanction is imposed, it is imposed in the amount minimum, in light of the extenuating circumstances indicated in this document.

Regarding that VDF "1) Acted in accordance with the Security Policy for contracting by private clients. To which he dedicates the First Allegation in based on the following arguments:

- That VDF could in no way know at the time of contracting that it was being possible to register without the consent of Mr.

Sources. This is so given that Vodafone's security procedure for private clients was guaranteed, since Mr. Fuentes was a client already existing in the Vodafone company, the contracting party was requested all the personal data required to carry out the processing of the hiring, that is, name, surnames and DNI.

- That VDF at the time of contracting, did have a cause

legitimizing to treat the data of the Complainant, in particular, the execution of a contract in which the interested party was a party (article 6.1 b) of the RGPD).

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

9/20

It should be noted that it is not true, as VDF alleges, that it could in no way understand or come to know that the person who made the telephone call has given place to the initiation of this sanctioning procedure was not Mr.

Sources, since in the documentation that VDF provides along with in its writing of August 12, 2021 it is known that VDF knew that the telephone line from which made the call did not belong to Mr. Fuentes, but belonged to another client different, being perfectly accredits the identity of the person who made said call, alleged fraudster, with name, surnames, DNI and telephone line from the that the call was made.

Therefore, VDF was able to know from the beginning that the line from which the The call was not from Mr. Fuentes, or at least suspected, so I shouldn't have allowed a different person from a different phone line than the legitimate owner, now a claimant, contracted a new terminal in his name mobile, and modify some of your personal data; and in addition, VDF issued the billing corresponding to the acquisition of the terminal to the now claimant. And it to Although VDF had adequate tools to identify from what line the call was being made and to whom that line belonged, and therefore could know from the beginning that the line from which the call was made was not from the

Mr. Fuentes and therefore, that the person who gave the consent was not Mr. Fuentes,

Therefore, VDF did not have the consent or any other basis for

legitimacy to carry out the treatment operations from which the

initiation of this sanctioning procedure.

In accordance with its security policy, VDF could in no case have asked the

person who made the call from a different phone line than the legitimate

holder, now claimant, the data that would be required from the holder of the line and that

supposedly they would have been the ones that the alleged fraudster would have facilitated. But,

under his own security policy, he should have required him to have

provided the customer service access code of the legitimate owner of the line

telephone company with respect to which the operations were being carried out, in such a way that

if the alleged fraudster had not provided said customer service access code

customer should not have been allowed to contract the new terminal, nor the

modification of the personal data of the complaining party, nor would the

bills. This shows that VDF would not have complied with its own policy of

security, having produced a failure in it.

For the reasons stated, the content of this allegation does not distort the facts or

the basis of law contained in the initiation agreement and must be dismissed

this first claim.

Regarding the request made by VDF regarding: "2) Subsidiarily, for the

In the event that the Agency understands that Vodafone has infringed article 6.1 of the

RGPD, the existence of culpability in the infraction imputed to

Vodafone and, consequently, no sanction can be imposed on the same. To

which dedicates the Second Allegation.

Indicate that VDF, after pointing out that it has not acted negligently, therefore

the imposition of any sanction would proceed, transcribes article 28.1 of the Law

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

10/20

40/2015, of October 1, on the Legal Regime of the Public Sector (hereinafter LRJSP), which includes the principle of culpability that governs the procedure administrative sanctioning and brings up the jurisprudence of the TS in relation to the exculpation and a sentence of the National High Court interpreting article 9 of the LOPD of 1999, allegedly in relation to cases in which a third party has accessed, through criminal activities, data of the interested parties guarded by a person in charge of the treatment, to try to justify that he does not attend the action of VDF any guilt, neither by way of fraud nor by way of fault.

Alleging VDF that it has acted at all times in compliance with due diligence that is required of him, not being able to impute any guilt to him, having used the diligence that was required to identify the applicant for a product or service in the telephone channel. Referring to what was stated in his First Allegation above, to prove that requirement.

First, to be exonerated as required by the Court's jurisprudence Supreme in relation to the acquittal, which VDF brings up in this allegation, by virtue of which "the invocation of the absence of fault will not suffice, but that it will be necessary to have used the diligence that was required by the person who claims its non-existence (among others, the Supreme Court Judgment of January 23, 1998 [RJ 1998\601])", VDF should have proved that in the present case acted with due diligence, albeit for the reasons already stated when responding to the allegation 1, it is not proven in this sanctioning procedure that VDF

has used the diligence that was required of him in relation to the claim that he has led to its initiation.

Second, we must disagree with the interpretation that VDF makes of the doctrine contained in the Judgment of the National Court (Chamber of Contentious-Administrative, Section 1) of February 25, 2010 [JUR 2010/82723]: that in relation to cases in which a third party has accessed, through criminal activities, to data of the interested parties guarded by a person in charge of the treatment, since there would be no "substantial identity", "in merit of facts, foundations and substantially the same claims", according to the settled jurisprudence of the Supreme Court in relation to the "substantial identity" (for all STS, Chamber Third Contentious-administrative, Section 6, Judgment of January 16, 2012, Rec. 4907/2011).

In the first place, the sentence cited by VDF differs in the facts since in it reference is made to a highly technical hacker who, breaking established security systems access a database and make a copy of the same, without any action having been carried out by the entity that suffers the security attack that indicates that said entity has made negotiations with the hacker that entail provision of services or modification of the data from the hacked database and made by the entity itself that has been object of the security breach.

While in the claim that has given rise to the processing of this sanctioning procedure would involve a third party, a VDF client, who by becoming go through the claimant, from a telephone line different from that of the claimant, and that VDF knew that it belonged to a different person (the telephone line from which the

C/ Jorge Juan, 6

28001 – Madrid

made the call is different from the phone line associated with the complaining party; you

VDF is aware that the telephone line from which the call was made belongs to another

person identified by their name, surnames and DNI) but hires on behalf of the

claimant party the acquisition of a mobile phone terminal, modifies the rates

that the complaining party had contracted and some of his identifying data;

all facts that VDF acknowledges that it knew, and, despite this, processes the request

made by the third party without the consent of the complaining party.

Secondly, the judgment cited by VDF differs in terms of the grounds,

since in this the infraction that would be imputed to the entity presumably

infringing would be a violation of the current article 32 of the RGPD, as it is understood that the

security measures that it had implemented were not adequate.

While VDF is charged with an infringement of article 6 of the RGPD, for having

carried out data processing (hiring a telephone terminal, issuing

of invoices, modification of rates, and certain personal data of the

claimant party) without the consent of the owner thereof, the claimant party.

Thirdly, the judgment cited by VDF differs in terms of the claims,

since what is sought by the appellant in the sentence is the annulment

based on the fact that it has not been specified or specified in the resolutions of the Agency

appealed the security conditions that have not worked to has not been

observed in the case.

While VDF claims in its allegations is the inadmissibility of the imposition

of any sanction agreeing the dismissal of the file with the consequent

file of the actions, for not having committed any of the infractions

imputed, that is, for not having processed the data without the consent of the party

claimant, or because the treatment is protected by some other basis of legitimacy.

In the aforementioned Judgment of the National Court of February 25, 2010, it states that:

Thus, even when article 9 of the LOPD establishes an obligation of result,

consisting of adopting the necessary measures to prevent the data from being

lose, misplace or end up in the hands of third parties, such obligation is not absolute and does not

can cover a case like the one analyzed. In the present case, the result is

consequence of an intrusion activity, not protected by the legal system and

in this illegal sense, from a third party with high computer technical knowledge that

breaking the established security systems accesses the database of

registered users at www.portalatino.com, downloading a copy of it.

And, such facts cannot be imputed to the appellant entity because, otherwise,

would violate the principle of culpability"

For the reasons stated, the content of this allegation does not distort the facts or

the legal basis contained in the initiation agreement, therefore, it must also

dismiss this second claim.

Regarding the third allegation of VDF "3) Subsidiarily to points 1) and 2)

above, and in the event that the Agency understands that there has been an infraction and must

impose a sanction on Vodafone, the circumstances must be taken into account

mitigating factors identified in the Third Allegation.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

12/20

Because it refers to mitigating and aggravating circumstances that are applicable to this

sanctioning procedure is considered more appropriate to respond in the fourth legal basis of this motion for a resolution containing such aggravating and mitigating factors.

III

In accordance with the evidence available at the present time of proposed resolution of the sanctioning procedure, and without prejudice to what result of the investigation, it is considered that the exposed facts do not comply with the established in article 6.1. of the RGPD, for which it could suppose the commission of a infringement typified in article 83.5 of the RGPD, which provides the following:

"Infringements of the following provisions shall be sanctioned, in accordance with paragraph 2, with administrative fines of a maximum of EUR 20,000,000 or, in the case of a company, an amount equivalent to a maximum of 4% of the global total annual turnover of the previous financial year, opting for the largest amount:

a) the basic principles for the treatment, including the conditions for the consent under articles 5, 6, 7 and 9;

[].»

For the purposes of the limitation period for infractions, the infraction indicated in the previous paragraph is considered very serious and prescribes after three years, in accordance with Article 72.1 of the LOPDGDD, which establishes that:

"According to the provisions of article 83.5 of Regulation (EU) 2016/679 are considered very serious and the infractions that entail a substantial violation of the articles mentioned therein and, in particular, the following:

b) The processing of personal data without the concurrence of any of the conditions legality of the treatment established in article 6 of the Regulation (EU)

2016/679.

(...).»

IV

In order to determine the administrative fine to be imposed, the provisions of articles 83.1 and 83.2 of the RGPD, precepts that indicate:

“Each control authority will guarantee that the imposition of fines

administrative actions under this article for violations of this

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

effective, proportionate and dissuasive.”

“Administrative fines will be imposed, depending on the circumstances of

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

13/20

each individual case, in addition to or as a substitute for the measures contemplated in the

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

administration and its amount in each individual case will be duly taken into account:

a) the nature, seriousness and duration of the offence, taking into account the

nature, scope or purpose of the processing operation in question

as well as the number of stakeholders affected and the level of damage and

damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor

to alleviate the damages suffered by the interested parties;

d) the degree of responsibility of the person in charge or of the person in charge of the

treatment, taking into account the technical or organizational measures that have

applied under articles 25 and 32;

e) any previous infraction committed by the person in charge or the person in charge of the treatment;

f) the degree of cooperation with the supervisory authority in order to put remedying the breach and mitigating the possible adverse effects of the breach;

g) the categories of personal data affected by the infringement;

h) the way in which the supervisory authority became aware of the infringement, in particular if the person in charge or the person in charge notified the infringement and, in such case, to what extent;

i) when the measures indicated in article 58, paragraph 2, have been previously ordered against the person in charge or the person in charge in question in relation to the same matter, compliance with said measures;

j) adherence to codes of conduct under article 40 or mechanisms certificates approved in accordance with article 42, and

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits realized or losses avoided, direct or indirectly, through infringement.”

Regarding section k) of article 83.2 of the RGPD, the LOPDGDD, article 76,

“Sanctions and corrective measures”, provides:

“two. 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 treatments of personal data.

C/ Jorge Juan, 6

- c) The profits obtained as a result of committing the offence.
- d) The possibility that the conduct of the affected party could have induced the commission of the offence.
- e) The existence of a merger by absorption process subsequent to the commission of the infringement, which cannot be attributed to the absorbing entity.
- f) Affectation of the rights of minors.
- g) Have, when not mandatory, a data protection delegate.
- h) The submission by the person in charge or person in charge, with voluntary, to alternative conflict resolution mechanisms, in those assumptions in which there are controversies between those and any interested party.”

In the present case, without prejudice to what results from the investigation, they have taken into account
In particular, consider the following elements.

-
-

The nature and seriousness of the violation, taking into account the purpose of the treatment operation in question as well as the level of damage and loss trials they have suffered; in accordance with the provisions of article 83.2.a) of the RGPD, since the personal data on which the availability has been lost position (temporarily), affect the remittance of a duplicate invoice with the personal data of the legitimate owner of the line, to the subscription of a contract deal for the acquisition of a mobile phone terminal that contained the data bank notes of its legitimate owner. These facts confirm the nature of the

infraction as very serious since it entails the loss of disposition and control over personal data.

The intentionality or negligence in the infringement; in accordance with article 83.2.b) of the RGPD, it should be noted that the degree of responsibility falls within the scope act of the claimed party and not of third parties, noting that the

SAN -Administrative Contentious Chamber- of May 5, 2021, establishes that:

“On the other hand, regarding the fact that we are faced with the fraud of a third party, as we said in the SAN of October 3, 2013 (Rec. 54/2012)-: "

Precisely for this reason, it is necessary to ensure that the person who hires is who really claims to be and appropriate prevention measures must be taken.

to verify the identity of a person whose personal data is

to be object of treatment”, not serving as an excuse that the third party that performs za fraud has managed to overcome the security policy of the claimed.

- Deny the concurrence of negligent action on the part of VDF equivalent to would acknowledge that their conduct -by action or omission- has been diligent. Ob-

Obviously, we do not share this perspective of the facts, since it has to be given evidence of lack of due diligence. It is very illustrative, the SAN of

October 17, 2007 (rec. 63/2006), assuming that they are entities

whose activity involves the continuous processing of customer data, including

states that “...the Supreme Court has understood that there is negligence

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

15/20

whenever a legal duty of care is disregarded, that is, when the in-

Fractor does not behave with the required diligence. And in the evaluation of the degree of diligence, the professionalism or not of the subject must be especially weighed. and there is no doubt that, in the case now examined, when the activity of the recurring one is of constant and abundant handling of data of a personal nature. nal must insist on rigor and exquisite care to adjust to the precautions legal tions in this regard"

- That it is a company whose main activity is linked to trafficking processing of personal data, in accordance with the provisions of article 76.2.b) of the LOPDGDD, The development of the business activity carried out by the claimed requires continuous and large-scale processing of personal data. end of customers. Being the one claimed positioned as one of the the largest telecommunications operators in our country.

On the other hand, the following have been taken into consideration, as mitigating factors:

- Article 83.2.c) RGPD:

☐ Measures taken by the person responsible to mitigate the damages suffered by the interested parties:

positive. Namely: Refund of the amounts charged for installments for the acquisition of the mobile terminal

- Article 76.2.c) LOPDGDD:

☐ The benefits obtained as a result of the commission of the infringement.

Obtaining an economic benefit beyond receiving the payment is ruled out. price of the cost fixed for the mobile telephone terminal, object of the fraudulent hiring. –

- Article 76.2.h) LOPDGDD:

The submission by the person in charge or person in charge, with

voluntary, alternative conflict resolution mechanisms, in those assumptions in which there are controversies between those and any interested.

Various telecommunications operators, including VDF, signed a Protocol with AUTOCONTROL that, without prejudice to the powers of the AEPD, provides mechanisms for the private resolution of controversies related to data protection in the field of contracting and advertising of communications services electronically, dated September 15, 2017. Protocol whose effective enforcement should be considered mitigating.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

16/20

To try to refute the aforementioned aggravating and mitigating factors, VDF dedicates the allegation 3 of his pleadings brief stating that in his Initiation Agreement, the Agency alludes to the graduation criteria of the sanction and performs certain value judgments that are not shared by Vodafone.

Thus, in relation to the nature and seriousness of the infringement, VDF indicates that the Agency, when categorizing the infraction as very serious, as the data included in an invoice, does not include in its analysis that the Fraudster already knew certain data of the Claimant, reason for which he was able to overcome the Security Policy of Vodafone and that, furthermore, in the present case there is only one affected (the Claimant).

Likewise, the Agency does not seem to take into consideration that all the

Relevant actions to ensure the security of the account prior to the notification of the claim by the Agency. Negotiations were carried out necessary to cancel the installment payment.

Second, in relation to intent or negligence, VDF alleges that the Agency, to quantify the sanction, does not assess the diligence and speed with which that my client processed, analyzed and resolved the claim filed by the woman of Mr. Fuentes.

Regarding the need to adopt "adequate preventive measures", it alleges VDF which, since March 14, 2012, acts under the Security Policy for the Recruitment of Individuals, which has been progressively updated, and whose The last modification has been implemented on January 4, 2022.

That said Security Policy establishes what type of information must be required to the client for each requested management; how to proceed in case a user does not exceeds said Policy, as well as preventive actions in situations of fraud.

And that it is mandatory for all employees and agents of Vodafone, who are responsible for applying and respecting it.

And that in this sense, in order to prevent similar incidents from occurring, Vodafone works continuously to improve Security Policies implemented in the contracting of services and in any other process that entails possible risks of fraud or irregular actions for our clients.

Likewise, Vodafone is reviewing its internal processes to ensure that the defined Security Policies are complied with or introduce the changes necessary when considered pertinent, in various areas of VDF's business.

Regarding the allegation in relation to the classification as very serious of the infraction It should be noted that VDF points out that it is because the data is affected in a invoice, but omits the subscription of a contract for the acquisition of a terminal of

mobile telephony that contained the bank details of its legitimate owner, everything that entails the loss of disposal and control over personal data.

In relation to overcoming the security policy, it should be noted that the

It is produced by a failure in it, since a third party, different from its

owner, overcoming said policy by providing the data that would be required from the owner of

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

17/20

the line and not the data that would be required in case you were not the owner of the line, as stated in its own security policy.

In relation to the assertion that the Agency in its initiation agreement has not taken

in consideration the pertinent actions carried out by VDF to guarantee the

security of the account prior to notification of the claim by the

Agency, and the necessary steps to cancel the payment in installments, must be

discarded since they have been taken into account as mitigating factors in the agreement of

start by virtue of the provisions of Article 83.2.c) RGPD.

The Agency does not share that VDF had to take 6 days from the time it became aware of

the alleged fraudulent acts until it took action in relation to the

themselves can be considered a diligent and rapid action, since VDF

could have adopted any other decision tending to block the proceedings

allegedly fraudulent before taking the definitive measures.

In relation to the allegation about the existence and content of the security policy

of VDF point out that it has been proven in this proceeding that the

It has not been fulfilled since it has been allowed to exceed it to a

person who was not the owner of a telephone line, providing the data required in the security policy for a holder.

In view of the foregoing, the following is issued

MOTION FOR A RESOLUTION

That the Director of the Spanish Data Protection Agency sanction

VODAFONE ESPAÑA, S.A.U., with NIF A80907397, for a violation of Article 6.1

of the RGPD, typified in Article 83.5 of the RGPD, with a fine of €70,000 (seventy a thousand euros).

Likewise, in accordance with the provisions of article 85.2 of the LPACAP,

informs that you may, at any time prior to the resolution of this

procedure, carry out the voluntary payment of the proposed sanction, which

will mean a reduction of 20% of the amount of the same. With the application of this

reduction, the penalty would be established at €56,000 (fifty-six thousand euros) and

its payment will imply the termination of the procedure. The effectiveness of this reduction

will be conditioned to the withdrawal or renunciation of any action or resource in via

administrative against the sanction.

In case you chose to proceed with the voluntary payment of the amount specified

above, in accordance with the provisions of article 85.2 cited, must do so

effective by depositing it in restricted account number ES00 0000 0000 0000 0000

0000 opened in the name of the Spanish Agency for Data Protection in the entity

banking CAIXABANK, S.A., indicating in the concept the reference number of the

procedure that appears in the heading of this document and the cause, for

voluntary payment, reduction of the amount of the sanction. Also, you must send the

proof of entry to the General Subdirectorate of Inspection to proceed to close

The file.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

18/20

By virtue of this, you are notified of the foregoing, and the procedure is made clear to you.

so that within TEN DAYS you can allege whatever you consider in your defense and

present the documents and information that it considers pertinent, in accordance with

Article 89.2 of the LPACAP.

BBB

INSPECTOR/INSTRUCTOR

926-260122

ANNEX LIST OF DOCUMENTS WORKING IN THE PROCEDURE.

Transfer of claim to VODAFONE ESPAÑA, S.A.U.

~

Claim of C.C.C.

~

~

Admission for processing to C.C.C.

~

Reply transfer of claim from VODAFONE ESPAÑA S.A.U

~

Writ of C.C.C.

~

Request additional information from VODAFONE ESPAÑA, S.A.U.

~

Response to the request from VODAFONE ESPAÑA S.A.U.

~

~

Agreement to initiate the opening of a sanctioning procedure against VODAFONE

Report previous actions.

SPAIN, S.A.U.

Information of the opening of the procedure to the claimant C.C.C.

~

~

Allegations to the start-up agreement of VODAFONE ESPAÑA S.A.U.

>>

SECOND: On April 19, 2022, the claimed party has proceeded to pay

the sanction in the amount of 56,000 euros making use of the reduction foreseen in the motion for a resolution transcribed above.

THIRD: The payment made entails the waiver of any action or resource in via against the sanction, in relation to the facts referred to in the resolution proposal.

FOUNDATIONS OF LAW

Yo

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

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

control authority and as established in articles 47 and 48.1 of the Law

Organic 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 Data Protection Agency.

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

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

19/20

II

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

Common to Public Administrations (hereinafter LPACAP), under the rubric

"Termination in sanctioning procedures" provides the following:

"1. Started a sanctioning procedure, if the offender acknowledges his responsibility, the procedure may be resolved with the imposition of the appropriate sanction.

2. When the sanction is solely pecuniary in 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 alleged perpetrator, in any time 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 infringement.

3. In both cases, when the sanction is solely pecuniary in nature, the competent body to resolve the procedure will apply reductions of, at least, 20% of the amount of the proposed sanction, these being cumulative with each other.

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 recourse against the sanction.

The reduction percentage provided for in this section may be increased regulations."

According to what was stated,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: TO DECLARE the termination of procedure PS/00611/2021, of in accordance with the provisions of article 85 of the LPACAP.

SECOND: NOTIFY this resolution to VODAFONE ESPAÑA, S.A.U.

In accordance with the provisions of article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure as prescribed by the art. 114.1.c) of Law 39/2015, of October 1, on Administrative Procedure Common of the Public Administrations, the interested parties may file an appeal contentious-administrative 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 in article 46.1 of the aforementioned Law.

C/ Jorge Juan, 6

28001 – Madrid

968-230522

www.aepd.es

sedeagpd.gob.es

20/20

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es