

□ File No.: EXP202206705

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 October 14, 2022, the Director of the Spanish Agency for
Data Protection agreed to start a sanctioning procedure against VODAFONE
SPAIN, S.A.U. (hereinafter, the claimed party), through the Agreement that
transcribe:

<<

File No.: EXP202206705

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 May 19,
2022 filed a claim with the Spanish Data Protection Agency. The
claim is directed against VODAFONE ESPAÑA, S.A.U. with NIF A80907397 (in
forward, the claimed party or Vodafone). The reasons on which the claim is based
are the following:

The claiming party states that on May 9, 2022 the claimed party
provided, without your consent, a duplicate of your SIM card to a third party other than the
owner of the line, which has led said third party, using the codes of
bank confirmation received on the affected telephone line, you have accessed your

bank account making unauthorized charges.

Along with the claim, the following is provided:

Screenshot related to the interaction carried out by the claimed party, in relation to with the duplicate SIM card.

Copy of the complaint filed with the Police on May 10, 2022.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

2/14

Copy of the invoice issued by the claimed party, on May 10, 2022, regarding the duplicate SIM card.

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 June 20, 2022 as

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

On July 20, 2022, this Agency received a written response from

Vodafone stating:

"A letter has been sent to the claimant through which we have proceeded to

inform you of the steps that were carried out by Vodafone to solve

the incidence.

In addition, they point out that the incident originated, as indicated by the claimant, because on May 9, 2022 a duplicate SIM was made on your mobile line

***PHONE.1 without your consent. This change was managed

by making a call to the Vodafone call center. In this sense, once

informed my client of the existence of a duplicate SIM obtained

Without the consent of the claimant, on May 10, 2022, Vodafone proceeded to

take all necessary steps to return control to the claimant

on your mobile line. In this regard, on the same day, May 10, 2022, the claimant

went to a Vodafone store where, after identifying himself, they processed a new

duplicate SIM and control over your mobile line was returned to you.

Likewise, Vodafone declared what happened as a fraudulent act on the 11th of

May 2022. Following the declaration of fraud, Vodafone proceeded to implement all

the necessary additional security measures by activating the victim check of

fraud on your Vodafone customer ID to prevent this incident from happening again

produce in the future and activated a pop-up window in your customer file in which

all Vodafone employees were informed of the following: "Do not provide

information, make modifications, product activation, orders, etc., if the client

calls from lines other than those you have contracted with Vodafone, concealment of

international call or origin. You should always consult and follow the policy of

security".

This part wants to point out that the effective management of a change of SIM card entails

the overcoming of the security policies that Vodafone has implemented in order to

prevent fraudulent practices on the personal data of their

customers. In this sense, and having processed said management subject to said policy

security, my client understood at all times that they were

lawful, real and truthful efforts.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/14

Vodafone works continuously to improve the Security Policies for its SIM change and duplicate processes, as well as for any other process that entails possible risks of fraud or irregular actions for our clients.

In this sense, since March 14, 2012, Vodafone acts under the Policy Security for the Contracting of Individuals, which has been updated progressively, and whose last modification has been implemented on the 4th of January 2022. Through said Security Policy, my client establishes what type of information must be required from the client for each requested management. In addition, It is included how to proceed in the event that a user does not pass the Privacy Policy Security, as well as preventive actions in fraud situations. The aforementioned Security Policy is mandatory for all

Vodafone After-Sales Services, who are in charge of applying and respecting it.

With regard to SIM card duplicates, it should be noted that the objective of Vodafone is that all duplicates or card changes are made face-to-face, since it is the safest way to guarantee that processes do not take place irregular or fraudulent and that, when the management to be carried out requires overcoming the Security Policy, the client must carry their original ID

To carry out a SIM change by telephone, it is necessary to carry out and exceeding the Vodafone Security Policy for such scenarios. Bliss Policy provides for three specific scenarios for which the change of card will proceed

SIM by telephone: (i) in those cases in which the platform in charge of the management of the change of the SIM card fails in such a way that the SIM change in our stores; (ii) if the client is a company and therefore prefers to make the change from platform 129/1442, sending in these cases the SIM card to the address of the company that appears in our systems; and (iii) if the client is prepaid and therefore the SIM card can be sent in cases of failure, loss/theft, incidence in the store and by customer request.

Likewise, and prior to verifying whether the applicant is under the scope of the three previous cases, the Customer Service Department of Vodafone, in accordance with said Security Policy, must invite you to attend to manage the change of SIM before a Vodafone After-Sales Service ("SPV") to give the maximum guarantee of security to the process. In case the client is find yourself in one of the three scenarios considered above, the Vodafone Customer Service Department will check prior to SIM change management that none of the following circumstances exist:

(i) there must not be any change of address in the last month; (ii) there must not have been requested previous SIM card shipments.

It should be noted that, in accordance with our Security Policies, the Compliance with any of the two previous requirements will lead to the need to process the SIM change in person at our stores. In those cases in which the applicant meets the requirements of the preceding paragraphs, the SIM change processing will depend on the following: (i) if the applicant calls from the same number for which you are going to request the SIM change, you will be asked for the access code of the Customer Service or DNI; however, (ii) if the client does not call from the same number, the telephone number associated with the

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

4/14

SIM ("MSISDN") together with the Customer Service access code or ID.

Additionally, it should be noted that all employees in the Department of Customer Service have received training on the steps to follow to carry out SIM changes, through the guide available to all agents on the portal called "REDPLANET", which includes all the processes and procedures of Vodafone that are applicable to them and the steps to follow in each case, according to the circumstances.

In any case, if the processing of a SIM change and/or a change of ownership exceed the previous Vodafone Security Policies, the carrying out such procedures in accordance with what is indicated in said Policies, when considering I represented the change as authentic, real and truthful. Not being able to represent me knowing that a third party stole the claimant's data without their consent. Without Notwithstanding the foregoing, as of May 10, 2022, my client carried out take the appropriate steps in order to protect the claimant as a client of Vodafone. In this sense, my client, at the request of the interested party, proceeded to declare what happened as a fraud, adopting the appropriate measures of security on your account, and to solve the different incidents that occurred with regarding the SIM card of the affected line.

Likewise, the claimant was reimbursed the amount of 5 euros for of duplicate SIM card expenses.

Therefore, by the time Vodafone was notified of this requirement, my

represented had already reestablished the services associated with the customer ID of the claimant and control over his line. Likewise, the processes are being reviewed to ensure compliance with the defined Security Policies or

Introduce the necessary changes when considered appropriate.

Specifically, my client is working on the continuous improvement of:

- Review of internal processes to ensure compliance with Security Policies and verification controls that have been defined and incorporated, both in channel face-to-face and by telephone, for duplicate SIM scenarios.
- Reinforcements periodic communication of Security Policies and verifications that have been defined by Vodafone for SIM duplicates and that must be applied by agencies, commercial stores and agents.
- Sending periodic communications to the face-to-face and telephone channel, as well as to the logistics operator, where it is alerted of the detected risk scenarios, their characteristics and behavior patterns to prevent new cases.
- Application -if applicable-, of the Penalty Policy existing for agents or distributors who make any duplicate or change of a SIM card without having required the documentation or that they carry out any management SIM change without following all the steps defined in the Security Policy.

Regarding the carrying out of transactions of the entity "BIZUM" of fraudulent nature revealed by the claimant in his claim, it is opportune to express that the change of a SIM card only implies access to the telephone line associated with it, and not the bank details of the holder.

Therefore, it does not seem possible that there is a correlation between the events that occurred in relationship with my client and what happened with the bank of which he is a client

www.aepd.es

C / Jorge Juan, 6

28001 – Madrid

the claimant. In this sense, the bank movements that he alleges in his claim do not have their origin, nor have they been caused by invoices for Vodafone services that he had contracted, but are due to accesses made through your bank account.

For this reason, Vodafone cannot be responsible for the accesses and bank movements that may have been made fraudulently. With all this, we can confirm that currently my client has carried out all the actions pertinent to solve the claim, estimating that it has been correctly resolved prior to the receipt of this document”.

THIRD: On August 10, 2022, in accordance with article 65 of the LOPDGDD, the claim presented by the claimant party was admitted for processing.

FUNDAMENTALS OF LAW

Yo

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

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

“personal data” as “any information about an identified natural person or identifiable (“the data subject”); An identifiable natural person shall be considered any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a name, an identification number, data of location, an online identifier or one or more elements of identity physical, physiological, genetic, mental, economic, cultural or social of said person;”

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

SIM. It is a smart card, in physical format and small in size, which contains a chip in which the service key of the subscriber or subscriber is stored used to identify itself to the network, that is, the mobile telephone line number of the MSISDN client (Mobile Station Integrated Services Digital Network - Mobile Station of the Integrated Services Digital Network-), as well as the personal identification number IMSI (International Mobile Subscriber Identity) subscriber

www.aepd.es

C / Jorge Juan, 6

28001 – Madrid

sedeagpd.gob.es

6/14

Mobile Subscriber-) but can also provide other types of data such as the information about the telephone list or the calls and messages list.

On the other hand, the issuance of a duplicate SIM card supposes the treatment of the personal data of its owner since it will be considered an identifiable natural person any person whose identity can be determined, directly or indirectly, in particular

by means of an identifier (article 4.1) of the GDPR).

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

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

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

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

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

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

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

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

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

SIM card (Subscriber Identity Module) that uniquely identifies

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

subject

to data protection regulations.

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

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

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

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

conditions:

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

for one or more specific purposes;

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

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

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

responsible for the treatment;

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

Physical person;

e) the treatment is necessary for the fulfillment of a mission carried out in the interest public or in the exercise of public powers conferred on the data controller;

f) the treatment is necessary for the satisfaction of legitimate interests pursued by the person in charge of the treatment or by a third party, provided that on said interests do not outweigh the interests or fundamental rights and freedoms of the interested party that require the protection of personal data, in particular when the interested is a child. The provisions of letter f) of the first paragraph shall not apply. application to processing carried out by public authorities in the exercise of their functions”.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

7/14

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”.

II

In the present case, it is proven that Vodafone provided a duplicate of the card SIM of the claiming party to a third party, without their consent and without verifying the identity of said third party, which has accessed information contained in the phone mobile, such as bank details, passwords, email address and others personal data associated with the terminal. Thus, the defendant did not verify the personality of the person who requested the duplicate SIM card, did not take precautions necessary for these events not to occur.

Based on the foregoing, in the case analyzed, the diligence used by the defendant to identify the person who requested a duplicate SIM card.

Well, it is accredited as recognized by the claimed party in its writ of response to this Agency dated July 20, 2022, << that the incident was originated, as indicated by the claimant, because on May 9, 2022 the ***PHONE.1 without your

made a duplicate SIM on your mobile line consent. Said change was managed by telephone through a Vodafone call center call. In this sense, once informed of my principal the existence of a duplicate SIM obtained without the consent of the claimant on May 10, 2022, Vodafone proceeded to carry out all those steps necessary to return control to the claimant over their mobile line. In

In this regard, on the same day, May 10, 2022, the claimant went to a convenience store Vodafone in which, after identifying himself, a new SIM duplicate was processed and he returned control over his mobile line.

Likewise, Vodafone declared what happened as a fraudulent act on the 11th of

May 2022>>

However, it should be noted that Sim Swapping is a fraud that allows you to impersonate identity by kidnapping the phone number by obtaining a duplicate of the SIM card.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

8/14

In any case, the operator must be able to prove that for this specific case have followed the verification protocols implemented when requesting a duplicate SIM card.

Well then, the result was that the defendant issued the SIM card to a third party who did not he was the owner of the line.

In view of the foregoing, Vodafone is unable to prove that this procedure.

In the explanation provided by the claimed party, it does not indicate which could have been the specific cause that led to the issuance of the duplicate, beyond some generic explanations. In any case, Vodafone has not been able to prove that for this case the procedure implemented by itself be followed, since that, if they had done so, the refusal of the duplicate of the SIM card.

Based on the foregoing, in the case analyzed, the diligence used by the defendant to identify the person who requested a duplicate SIM card.

In accordance with the evidence available at this procedural moment and

without prejudice to what results from the investigation of the procedure, it is estimated that the conduct of the claimed party could violate article 6.1 of the GDPR and may be constituting the offense classified 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.

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

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

Article 58, paragraph 2, letters a) to h) and j). When deciding to impose a fine administration and its amount in each individual case shall be duly taken into account:

- a) the nature, seriousness and duration of the offence, taking into account the nature, scope or purpose of the processing operation in question, as well as such as the number of interested parties affected and the level of damages that have suffered;
- b) intentionality or negligence in the infringement;
- c) any measure taken by the 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, having given 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. certifications 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.

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.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

10/14

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 factors:

-

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

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

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

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

with respect to entities whose activity entails the continuous processing of

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

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

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

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

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

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

handling of personal data must insist on rigor and exquisite

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

As mitigations:

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

effective (art. 83.2 c).

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

11/14

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 VODAFONE SPAIN,

S.A.U. with NIF A80907397, 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 VODAFONE ESPAÑA, S.A.U. with NIF

A80907397 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.

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
www.aepd.es

C / Jorge Juan, 6

28001 – Madrid

sedeagpd.gob.es

12/14

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.

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 November 25, 2022, the claimed party has proceeded to the payment of the penalty in the amount of 56,000 euros using one of the two reductions provided for in the Commencement Agreement transcribed above. Therefore, there has not been The acknowledgment of responsibility has been accredited.

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

FUNDAMENTALS OF LAW

Yo

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

13/14

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."

According to what has been stated,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: DECLARE the termination of procedure EXP202206705, in accordance with the provisions of article 85 of the LPACAP.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

14/14

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 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

937-181022

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es