 File No.: PS/00281/2021

RESOLUTION OF SANCTIONING PROCEDURE

Of the procedure instructed by the Spanish Data Protection Agency and with

based on the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the claiming party) files a claim with the

Spanish Data Protection Agency (AEPD) dated 02/25/2021.

The claim is directed against VODAFONE ESPAÑA, S.A.U., with NIF A80907397 (in

forward, the claimed party or VODAFONE). The claim is based on the fact that the

claimed has registered a prepaid telephone line associated with the NIF of the

claimant, who denies having hired her; have consulted the information system

EQUIFAX credit card using the NIF of the claimant as search criteria

despite not having a legitimate interest for such treatment; has not attended

rights of access and deletion exercised by the claimant and has responded to their

deletion request that, since there is a line linked to your NIF, "you will not be able to delete

your data until the expiration date of the line does not arrive as long as the

owner does not carry out any recharge".

The claimant has provided annexes to the claim with these documents:

1. Copy of eight emails you exchanged from your email address,

***USER.1@gmail.com,

address

derechosprotecciondatos@vodafone.es.

VODAFONE

with

in

the

1.1.- Dated 12/19/2020, sent by the claimant, in which she requests access to

your data that may appear in the VODAFONE records and with which it sends you

a copy of your ID.

1.2.- From 12/21/2020 at 7:20 p.m., sent by VODAFONE, in which he responds

that, in view of your request for access, in accordance with article 15 of the GDPR,

“We regret to inform you that you are not entitled to obtain the right

of access with respect to personal data (National Identity Document)

that appear in the VODAFONE ESPAÑA system since you do not register in the

himself as the owner of the required data. We remind you that, if you wish, you can

exercise your rights of deletion, access, limitation, rectification and portability

by sending a written communication, accompanied by a copy of your ID or

equivalent identification document, to the address [...]” (The underlining is ours)

1.3.- From 12/21/2020 at 8:21 p.m., sent by the complaining party with this text:

"A complaint filed with the national police due to a usurpation of

my identity, for which I am requesting access to the personal data that

may appear related to my ID or name, since you have consulted

my data on 09/15/2020 18:40:27 in an Equifax file illegitimately

I have no contract or relationship with you." The claimant refers to the



requested a copy of the police report, your ID and your request to exercise the

Right of access.

1.4.- From 12/29/2020, sent by VODAFONE with an identical response to that of the

electronic message sent to the claimant on 12/21/2020.

1.5.- Of 01/24/2021, sent by the claimant, in which she exercises the right to

deletion of your data. The text is the following: "This email is sent to request the

deletion of my data from their databases, since they do not provide me with the

information related to my ID, and they should not have any of my data since

I have no relationship with Vodafone. Attached:

-Application signed. -DNI -And expansion of the complaint in which it has been provided to

the national police the information that they indicate to me together with that of other companies. [...]"

1.6.- Of 01/26/2021, from VODAFONE, in which it responds:

"[...] In view of your request, in which you exercise the right to delete your data

personal in accordance with article 17 of Regulation (EU) 2016/679 [...]

We regret to inform you that this entity cannot generate the deletion of the

data requested since they are necessary to provide the service to the line

prepaid ***PHONE.1, we understand the purpose of your request, however and

In case of not recognizing the product we could generate a rectification of data

so that the service is in your name and you can use it; we emphasize

that prepaid products cannot be deactivated, failing that we can

wait for the card to expire (approximately the expiration date is estimated at

June 2021 if recharges are not generated), after that it could require again

your right of erasure." (The underlining is ours)

1.7.- From 02/01/2021, from the claimant, with this text: "[...] They tell me from the channel

from Vodafone Spain from facebook who opened petition number 10915XXXX to

fraud department, where they notify that there is indeed an error and that it is

solved. Can you confirm the deletion of my data? [...] "

1.8.- From 02/03/2021, sent by VODAFONE, in which it says that "[...] In response to

your email, we must inform you that the line ***TELEPHONE.1 corresponding to the

file registered with your National Identity Document number has expired

by our fraud area in order to avoid any type of use, however

it still registers in our system and will only be disconnected until the month of

June 2021, which makes it impossible for your data to be deleted from our system.

However, the data protection department generates a general statement

alerting all our areas to omit any type of management on the file

fraudulent, annexed to it we generate the opposition to the treatment and use of the data with

commercial purpose.

Finally, we make the clarification that your request (Deletion of data) only

It can be attended until the date previously stated (June 2021), therefore

It is necessary that you send us this request at the end of the month indicated.

We remind you that, if you wish, you can exercise your rights of access, rectification,

limitation, opposition and portability by sending a written communication,

accompanied by a copy of your ID or equivalent identification document, to the address

[...]" (emphasis added)



2. Copy of the complaint filed at the police station on 12/11/2020 and the

Extension of complaint dated 01/23/2021.

2.1. Complaint of 12/11/2020 (Certificate XXXXX/20) in which the claimant exposes the

events that occurred on 11/12/2020: when activating the credit card of the financial institution

ING receives a text message denying activation as it is included in the

file BADEXCUG. After consulting the reason for inclusion, since it does not have any debt, they respond that there is an outstanding debt derived from a purchase carried out on the internet with the company Sequra for an amount of XXX.XX€. contact with that company, which sends you a copy of a contract with your personal data if well the second last name and the letter of the DNI are wrong. The claimant informs them that she has not made any purchase and they answer that she should file a complaint in the police.

To questions from the agent who draws up the report, he states that he has not lost his documentation and that the data could be obtained from the BOE since it has requested several scholarships and their data have been published with the same error. To the question of agent regarding whether something similar had happened to him previously, he replies that tried to register through his mobile application in the chain "(...)" and reported that there was already another person discharged with his name, but he did not give importance.

2.2. Certificate XXX/21. This complaint is an extension of "the initial XXXXX/20 of 09/11/2020 and extension of XXXXX/20 of 12/15/20". The complainant provides, in relation to the phone that was allegedly purchased with your personal data, the following data used by the perpetrators of the act provided by the company with the one that supposedly hired: email ***USER.2@outlook.com. Date birth 08/17/19XX.

3. A document with the EQUIFAX anagram, dated "11/12/2020", with the result of the searches carried out by the identifier NIF ***NIF.1 (the one of the claimant) In the section "Operations in the Asnef file", there is no data. In it In the "History of queries" section, a query made on 09/15/2020 at 18:40.27.8. by Vodafone Ono, S.A.U.

4. Various screenshots obtained from the page that VODAFONE has on

Facebook with fragments of the conversation held through the chat between

both. The claimant says: "you can consult the email thread that I kept with

Vodafone data protection. I sent them a photocopy of the ID, police report

and they have false data in their databases [...]". The defendant answers: "What do you

It seems if we review your case from here? Provide us with your customer information (name,

surnames, telephone and ID) to be able to manage what you need. The claimant

warns that she is not a client of the operator and refuses to provide any

document, despite the insistence of the requested entity. The last catch of

screen includes the response of the defendant in which she states that, from the

fraud department, "through the request we sent yesterday no.

10915XXXX, they have classified it as an error, which from said department they have

remedied." The date of 01/31/2021 is recorded.



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), the claim was transferred to the defendant so that

proceed to 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.

On 07/05/2021, the response from VODAFONE was received stating that it has

communicated to the claimant that, on 05/27/2021, she has complied

effective to your right of erasure. Provide a copy of the letter dated 06/25/2021

addressed to the claimant (document annex 1) in which, although it informs her of the

deletion of your data there is no reference to the date of 05/27/2021.

The defendant responded to the transfer actions carried out by this Agency in

the following terms:

1.About the causes that led to the incident that gave rise to the claim,

“confirms” that on 12/19/2020 the claimant exercised the right of access to her data and

who responded on 12/21/2020 informing him that "she is not legitimized to

obtain the right of access with respect to personal data (Document

National Identity) that appears in the system of my [the defendant] since Mrs.

[the claimant] is not registered as the holder of the required data.” "This is because

because the data of Mrs. [the claimant] were related to a third party who

used the data of the Interested Party fraudulently. In this case, the only data

the claimant's staff that is related to this fraud is the DNI, reason why

which in the evidence that is provided of the systems of my represented appears

information from a third party "B.B.B.", with the DNI of the claimant ***NIF.1.” Add that

the claimant exercised the right of access again on 12/21/2020 and that he responded

in the same terms of your reply dated 12/21/2020.

In addition, it acknowledges that the claimant requested the deletion of her data and that

responded on 01/26/2021 that "in this case, the service contracted and related to

your data is a prepaid service, which means that once issued it will not be

You can unsubscribe until it expires. In this regard, Ms. [complainant] is advised

that the service is scheduled to expire in June 2021.”

It states that the claimant went to Facebook and that she was informed through this channel that she was

had informed the Fraud department of the company to analyze his

case; that, after receiving this information, the claimant sent him an email on 02/01/2021

requesting the deletion of their data to which the defendant responds on 02/03/2021

“informing the [claimant] that the case has been registered as fraudulent for

avoid any further use of your data. However, you are informed that

the line, being prepaid, cannot be disconnected until June 2021, which

that makes it impossible for the data of the Interested Party to be deleted from the system of my

represented.”

2. Regarding the measures adopted to prevent incidents from occurring

similar, VODAFONE responded that the events "have been caused by fraud

from a third party by overcoming the security policies of [the claimed carrier]

satisfactorily, because to carry out the registration of a prepaid line, the



display of an official identification document to store agents

of [the claimed operator].” Indicates that he was not aware of the existence of this

fraud until notified by the claimant and that at that time "it was

initiates a procedure to verify the facts and remedy the situation.” (He

underlined is ours)

It states that, as a consequence of this process, the Fraud department classified

the situation as fraudulent and generated a general statement alerting all

the areas of the company to omit any type of management on the file

fraudulent.

The attached document 3 that VODAFONE has provided reflects the information contained

in the tab "Info. of Contact", linked to the NIF of the claimant, which is associated

to the name of B.B.B., in which under the heading "Form>Notice Detail" appears this

legend: “Do not generate changes to this file. Do not register any type of product,

is classified as fraud. The data registered in the client are erroneous and

belong to another user.” (The underlining is ours)

3. The defendant declares that it has complied with the request of the claimant to delete

their data from their systems, "prior blocking of the data of the interested party" and contributes to such

order, in addition to the letter that he addressed to you on 06/25/2021 (annex document 1), as

attached document 4 various screenshots with the following information:

In the "Customer registration" tab, the reference appears with the "Order number V"

***REFERENCE.1; as "Title" "Prepaid Installation With..." and as "F. Opening"

“11/17/2020”. In the lower box, "Requests, claims, breakdowns", are recorded

several claims, including one dated 01/26/2021 with this information: As

“Type”, consists of “Fraud”; as "Code", "possible fraud" and as "Subcode",

"Impersonation".

In the tab "Info. Contact" contains the NIF of the claimant. A screen

pop-up asks if you want to perform the data cancellation action for that NIF

and the option “yes” is marked on it. In the following screenshot a message

popup says no contact found matching the criteria

search.

THIRD: On 06/2/2021, the claim made by the

claimant. In accordance with article 65.5 of Organic Law 3/2018, of 5

December, protection of personal data and guarantee of rights

(LOPDGDD), that decision was notified to the claimant on 06/2/2021.

FOURTH: Initial agreement.

On 02/03/2022, the Director of the AEPD agrees to start the procedure

sanctioning VODAFONE in accordance with the provisions of articles 63 and 64 of the

Law 39/2015, of October 1, on the Common Administrative Procedure of

Public Administrations (hereinafter, LPACAP), for the alleged infringement of the

articles 6.1. (two infractions) 15 and 17 of the GDPR, typified, respectively, in the

Articles 83.5.a) and 83.5.b) of the GDPR.



The startup agreement was notified to VODAFONE electronically, as planned

in the LPACAP as evidenced by the certificate issued by the FNMT that is in the

proceedings.

FIFTH: Request for extension of term and copy of the file.

By letter received at the AEPD on 02/14/2022, VODAFONE requests that

extend the period initially granted to make allegations and that it be delivered

a copy of the file.

The AEPD, by means of a letter that the defendant received on 02/21/2022, notifies her that

grants, for the maximum allowed by article 32.1 of the LPACAP, the extension of

period requested and sends you a copy of the documentation.

SIXTH: Allegations to the initiation agreement.

On 02/28/2022 VODAFONE presents its allegations to this Agency to the

opening in which, in relation to the infringement of article 15 of the GDPR, requests

"Have recognized the responsibility of Vodafone Ono, S.A.U."

Regarding the remaining violations of the GDPR that were attributed to him in the agreement of

initiation - violation of articles 6.1. and 17 of the GDPR- denies its commission and requests

the dismissal of the file with the consequent archiving of the proceedings.

Subsidiarily, in the event that a sanction is imposed, it requests that it

set at the minimum amount in application of the mitigating circumstances whose concurrence it invokes.

In support of its claims, it alleges the following:

1. First, he delimits "the object of the debate" and makes a list of what he considers

are "some facts, stripped of any legal assessment, which we understand to be

are relevant and should be taken into account when deciding on the taxation of

sanctions against Vodafone and, if necessary, on their amount.":

<<1. The facts refer to a single interested party (the Complainant) who is not

Vodafone customer.

2. The only personal data of the Claimant that was processed by Vodafone was the

Regarding your National Identity Document ("DNI"): ***NIF.1.

3. Said personal data is available, along with the name and surname

of the Claimant, (…).

4. On September 15, 2020, Vodafone made a query in the

credit information and Equifax with the Claimant's DNI. Likewise, in

September 2020 up to a total of five different entities carried out

inquiries to Equifax with said NIF. Four of these consultations were carried out on 16

September 2020, one day after the one carried out by Vodafone.

5. On November 17, 2020, a third party, under the name of B.B.B. (he

"Third Party"), registered a prepaid card using the DNI number of the

claimant.

6. The prepaid card was not registered in the name of the Claimant, but of the

own Third.

7. The Claimant's DNI number, as she herself admits and as stated

accredited in the file, has been used for third parties to hire or

try contracting other services and make purchases that have nothing

to do with Vodafone.

8. As Claimant admits, identity theft does not occur

as a consequence of Vodafone's conduct, but prior to the

Third Party contact with Vodafone: "After requesting access to various files

of defaulters due to identity theft, it is observed that Vodafone

ONO SAU has consulted my DNI in ASNEF Equifax.>> (The underlining is

our)

2. The issues on which VODAFONE pronounces itself in its writ of

allegations to the start agreement are these:

(i) VODAFONE "has not infringed article 6.1 of the GDPR in any of the

data processing identified in the Initiation Agreement": A) Registration of the mobile line

prepayment "in the name of the claimant"; and B) consultation of an information file

linked to the claimant's DNI.

(ii) Secondarily, in the event that the AEPD understands that there has been

offense, alleges that "there is no fault in the offenses charged [...] and, in

Consequently, no sanction can be imposed."

(iii) VODAFONE has acknowledged responsibility for the violation of article 15 of the

GDPR regarding the right of access.

(iv) VODAFONE denies having infringed article 17 of the GDPR, regarding the right to

suppression.

(v) Secondarily, "in the event that it is understood that Vodafone has infringed

articles 6.1 and/or 17 of the GDPR and, in the case of infringement of article 6.1,

considers that a sanction can be imposed on the claimed party, they must take into account

into account the extenuating circumstances" that he invokes in the sixth allegation of his

written.

The considerations that VODAFONE makes on each of the issues

These are, in summary, the following:

(i) 1. Violation of article 6.1. of the GDPR: registration of the prepaid mobile line in the name

of the claimant.

He begins by exposing what, in his opinion, is the position held by the AEPD in the

startup agreement.

"The Agency understands that "the treatment of the NIF of the claimant linked to the

contracting a prepaid line in the name of B.B.B. [the Third Party], line that the

claimed registered on November 17, 2020, was not founded in

none of the legitimizing circumstances of the treatment provided for in the

article 6.1 GDPR", and that therefore the precept would be infringed.

Continuing with its argument, the Agency affirms that Vodafone "must be able to

certify that the person with whom you contracted and identified with certain

personal data -particularly the NIF of the claimant- was effectively his

owner", as well as that Vodafone "has not provided any evidence that proves



that, when contracting the line associated with the claimant's NIF, he acted

with the diligence that is required in compliance with the principle of legality; principle

which it is obliged to respect and compliance with which it must be able to demonstrate".

According to the Agency, the "mere display of an identification document [...]

constitutes a clearly ineffective and insufficient measure".

Next, it makes this "clarification": that the third party that intervened in the contracting

he did not contract the line "in the name of the claimant" but in his own name.

"First of all, we want to clarify that we are not dealing with a case of

identity theft in which a third party has contracted a line or

requested a duplicate SIM card "in the name of the claimant" (this is stated

manifestly erroneous and untrue, for example, in the

pages 31 and 42 of the Commencement Agreement). What has happened is that the Third,

using the claimant's DNI number, has registered a card

prepaid in your own name, not the claimant's.

In other words, the owner of the prepaid mobile line is the Third Party, not the

claimant." (The underlining is ours)

Finally, VODAFONE denies having violated the principle of legality and considers that it

was entitled to process the NIF data of the claimant that the third party that

intervened in the recruitment facilitated. It does the following on the individual

statements:

Contrary to what the Agency thinks, Vodafone understands that it was

legitimized to process the personal data used by the Third Party – applicant

of a prepaid card –, including the ID number provided, question

Another thing is that the DNI data processed did not correspond to the Third Party, who is the one who

contract the prepaid card. Although we do not share the interpretation –

too strict, in our opinion – of the legitimizing legal basis of the

Article 6.1 b) of the GDPR that the Agency makes in the last paragraph of the page

legal

15 of the Initiation Agreement, it turns out that the basis

legitimizing that protects the

treatment of Vodafone is indicated in article 6.1 c) of the GDPR: the

compliance with a legal obligation.

This legal obligation is found in the Sole Additional Provision of the Law

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

electronic communications and public communications networks (the “Law

25/2007”), which establishes that:

"1. Mobile telephone service operators that market services

with activation system through the modality of prepaid cards,

must keep a book-registry in which the identity of the clients that

acquire a smart card with said payment method.

Operators will inform customers, prior to the sale, of the

existence and content of the record, its availability under the terms

expressed in the following number and the rights included in the article

38.6 of Law 32/2003.

The identification will be made by means of a document accrediting the

personality, recording in the registry book the name, surnames and

nationality of the buyer, as well as the number corresponding to the document



identification used and the nature or name of said document. In it

case of legal persons, the identification will be made by providing the card

of fiscal identification, and the denomination will be recorded in the book-registration

social and tax identification code".

The defendant ends its argument with this statement:

"Vodafone is obliged by Law 25/2007 to treat the "corresponding number

to the identification document used" by the buyer of the prepaid card;

A different matter is that said number turns out to be wrong or has been used

through fraud by a third party, but this may not imply, in any case,

a violation of article 6.1 of the GDPR."

On the "degree of diligence" that he displayed in relation to the conduct that he has given

origin to the infringement of article 6.1 of the GDPR that was attributed to him in the agreement of

opening (registration of a prepaid line linked to the NIF of the claimant), considers that

It was the "right" one. Thus, it says: "In any case, the measures adopted by

Vodafone to prove the identity of the prepaid card applicant are not

ineffective or insufficient." (The emphasis is ours) In defense of that position

adduces:

"We believe it convenient to take as a starting point what is required by the legislation,

which we understand is the yardstick that should be taken by Vodafone and

the rest of the operators.

In the first place, the aforementioned Law 25/2007, a rule directly applicable to

Vodafone, indicates that mobile phone service operators that

commercialize prepaid cards must prove the identity of the customers who

acquire one of these cards "through a document accrediting the

personality, recording in the registry book the name, surnames and

nationality of the buyer, as well as the number corresponding to the document

identification used and the nature or name of said document".

The norm does not require that a copy of the DNI be kept, but only of the data that

in the document provided.

Likewise, although Organic Law 5/1985, of June 19, of the Regime

General Electoral, it is not applicable to the case, it does serve as a button

of sample in order to demonstrate that the exhibition of a DNI is sufficient to

identify the person who is going to exercise one of the fundamental rights for

antonomasia, the right to vote."

VODAFONE adds that "the identification obligation has been duly

transferred by that entity to its wholesaler, Sercom Soluciones, S.L. ("Sercom") that, to

in turn, signed an agreement with the point of sale that registered the prepaid card to the

Third." We refer to the stipulations of the contracts entered into between

VODAFONE and SERCOM and between the latter and the point of sale

***ESTABLISHMENT.1 that are reproduced at the end of this Antecedent.

Continuing with the question of the diligence that it claims to have deployed, the defendant

Add:

"For the rest, in its Commencement Agreement the Agency would be demanding Vodafone

and, by extension, to thousands of Vodafone points of sale and the rest of

telephone operators, to implement, for example, a software for



scanning and verification of DNIs: "The mere display of a document

identification, to which the defendant alludes - she affirms that the third party who contracted

exceeded company security policy by displaying the document

identification - constitutes a clearly ineffective and insufficient measure that is

far below the possibilities that current technical development offers and that

does not take into account the obvious risk that the contracting of services that
The claimed commercializes represents for the rights and freedoms of the
people".
The foregoing means demanding from Vodafone a degree of diligence totally
excessive and outside the market standard: not only is it superior to the
standards dictated by the applicable regulations (we refer to Law 25/2007),
but it is not followed even in actions as sensitive as exercising
the right to vote.
Having said this, if the Agency intends to increase the requirements in terms of
identification incorporating conservation obligations and technical verification
of documents, what proceeds is to approve rules to that end but, in no case,
Vodafone may be accused of negligence or lack of soundness of the measures
taken at this time, but first the aforementioned
rules and later, if applicable, penalize the operator that does not
apply, but what is not in accordance with the law is to try to use directly
the disciplinary route as a method of setting security parameters
demandable.
In fact, in this particular case there is no possibility for the
private operators to check if the ID number corresponds
effectively to the person who claims to be the owner and accredits it with a document
that can be manipulated. Otherwise, it would go against the regulations of
data protection, and that is that the only way to avoid fraud like the one that has
origin of this file would be that Vodafone had access to a database
data that would allow verifying that if the ID number used by the
applicant actually belongs to the applicant in question." (The underlining is
our)

2. Violation of article 6.1 of the GDPR: consultation of the EQUIFAX file linked to the

NIF of the claimant made on 09/15/2020.

VODAFONE denies the alleged infringement and thus summarizes the position held by the

AEPD in the opening agreement:

“The Agency considers that: 1. There is no evidence linking the consultation

made to Equifax on September 15, 2020 with the registration of the prepaid line

made on November 17, 2020, [...]. 2. In the event that the consultation does not

was linked to the registration of the prepaid line, Vodafone would not have

"provided information about the origin of the data processed and about what was the

reason for the consultation", so the treatment could not be classified as

"legitimate" in the sense of article 20.1 e) of the LOPDGDD.”



Next, he dedicates a specific section in his pleadings brief to underlining

that "the Claimant's ID number was used to carry out a multitude of

consultations": "As has been proven in the file, the number of the

Complainant was used by different actors (including Vodafone) to carry out

several consultations in mid-September”. He incorporates into his writing a relationship of

queries to the EQUIFAX file (a total of nine) made by seven entities

using as search criteria the NIF of the claimant during the

period of time between 06/19/2020 and 09/16/2020.

The defendant denies that consulting the EQUIFAX file constitutes an infringement

of the data protection regulations and maintains that "it was carried out respecting the

provided in article 20.1 e) of the LOPDGDD" and was related to "a

online request".

Regarding the "online request" linked to the NIF of the claimant that she allegedly received

It does not provide any document that proves its existence. The information you provide

on the aforementioned "online application" consists of the statement that the product

on which the contracting request was concerned implied financing, payment

deferred or periodic billing, to conclude without further ado that the treatment was

included in the scope of application of article 20.1 e) of the LOPDGDD.

Next, he explains the differences between the registration of prepaid and postpaid products to

purposes of examining the creditworthiness of the client. It says that "registration of prepaid cards does not

they imply a process of scoring and consulting delinquency files. sayings

processes (including inquiry to Equifax) only apply to financings or

Vodafone products that involve deferred payment or periodic billing."

For the purposes of proof, it provides as documents 5 and 6, the "General Conditions of

Mobile Communications Services. Prepaid" and the "General Conditions of

Postpaid Mobile Communications Services. Individuals", respectively, and

indicates that its reading allows us to verify that, while those relating to services

postpaid, information is provided on the possibility that this entity verifies the solvency

of the client by means of consultations to patrimonial solvency and credit files

("Vodafone may verify the solvency of the Client through procedures

automated "scoring", by obtaining data from the entities

bank accounts provided by the Client or through asset solvency files and

credit"), this possibility is not mentioned in those relating to prepaid services.

For greater clarity, the following fragment of their allegations is transcribed:

"On September 15, 2020, Vodafone consulted the file

ASNEF with the DNI [...]. This query is in no way linked to the

prepaid card registration that took place in November 2020, two months

later, but with an online request. In this sense, the registration of cards

prepaid do not imply a process of scoring and consulting files of

late payment Such processes (including inquiry to Equifax) only apply to

financing or Vodafone products that involve a payment

deferred or periodic billing.[..]" (The underlining is ours)



In short, the defendant denies the commission of the two violations of article 6.1 of the

GDPR that was attributed to him in the agreement to start the file and says that "In

Consequently, the sanction proposed by the Agency cannot be imposed on Vodafone."

(ii) Subsidiarily, in the event that the AEPD understands that there were

the infractions that the defendant denies, it is alleged to the contrary that it is missing in both

cases the necessary element of guilt, which would prevent this Agency

penalize those behaviors.

1. The defendant affirms that she has acted at all times in compliance with the diligence

that it is required of him, that his conduct is not guilty, neither by fraud nor by

fault title.

He states that he has used the diligence that was required of him to identify the

prepaid card applicant because "has complied with the provisions of the Law

25/2007."

It invokes as a basis article 28 of Law 40/2015, of the Legal Regime of the

Public Sector (LRJSP), which proclaims the principle of guilt in the field of

disciplinary administrative procedure and requires that the offending party be

responsible by way of fraud or negligence, and also refers to the judgment of the Court

Supreme Court of January 23, 1998 [RJ 1998\601]) in which the Court states that

"for the exculpation, the invocation of the absence of guilt will not suffice, but it will be

It is necessary that the diligence that was required by the person claiming their

nonexistence."

It adds that "the National Court has understood, in 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 (this is not the case, Vodafone did not keep the data of the

Complainant), that imputing such facts to the data controller could lead to

the violation of the principle of guilt." For this purpose, the SAN, Chamber of the

Administrative Litigation, Section 1, of 02/25/2010. In consideration of what

exposed says: "In this case, we are dealing with a criminal practice carried out by

a third party who, acting fraudulently, has provided the ID number of a third party to the

request the registration of a prepaid card in their own name, passing the controls

established by Vodafone. Then, if the previous jurisprudence has resulted from

application in cases in which the data of the interested parties were guarded by the

responsible for the treatment, all the more reason it should also be applied to those

other cases in which the duty of custody does not weigh on the person responsible (who

can more, can less).

2. It alleges that, in this case, the processing of personal data of the claimant

"It has been due to the existence of human error, which are unavoidable and on which

Vodafone cannot have effective control." Argue the following:

"[...] there may be cases, such as this one, in which Vodafone processes data

personal that does not belong to the prepaid card applicant, but to a third party

(the Claimant). This is what has happened in this case: it is evidence and it is not

we deny.



In these (residual) assumptions, we would be faced with assumptions in which the applicant (the Third Party), using tricks and using in his favor his criminal experience, has managed to evade the controls established by Vodafone, causing human error at the Point of Sale.

The Agency has ruled on numerous occasions on the errors humans, stressing that they cannot be punished. For example, in the Disciplinary Procedure PS/00210/2019 and in the Procedure E/02877/2019, in which the Judgment of the National Court (Sala de Litigation, Section 1) of December 23, 2013 [JUR 2014\15015], in which in turn highlighted that: "The question, then, must be resolved in accordance with the principles of punitive law given that mere human error does not can give rise, by itself (and above all when it occurs with character isolated), to the attribution of penalizing consequences; So, if it's done like that, it would incur in a strict liability system prohibited by our order constitutional".

And add below:

"In addition, if the National Court and the Agency have considered human error as excusable in cases in which there was no external element that induces the natural person in question to incur the error, all the more so should the excusability of it be appreciated when it has

been a third party who, through criminal intent, has directly induced the

mistake." (The underlining is ours)

(iii) VODAFONE has acknowledged responsibility for the violation of article 15 of the

GDPR regarding the right of access. The defendant stated in this regard:

“As we have advanced in the previous Allegation, Vodafone

acknowledges its responsibility solely and exclusively for the violation of article

15 of the GDPR, which should entail a reduction of 20% of the

proposed sanction for this offense (100,000 euros). Also, in case of

that the payment be made before the resolution of this procedure, the

penalty should be reduced by an additional 20%, the amount to be paid being

60,000 euros.”

(iv) VODAFONE denies the infringement of article 17 of the GDPR derived from not having

proceeded to suppress the NIF data of the claimant when she exercised this

right.

He alleges that he acted correctly and that there is no violation of article 17 of the GDPR. TO

purpose of its response to the deletion of the NIF data requested by the claimant,

recognizes that the "wording" was "unfortunate" and says that what is relevant for the purposes of

Determining whether article 17 of the GDPR has been infringed is not so much the answer that is

provided to the claimant - "we do not deny that it was unfortunate" - but

respect on your part of the applicable regulations.

In defense of the fact that his action was in accordance with article 17 of the GDPR, he argues the

following:

1.First of all, consistent with your first allegation, in which you deny the

violation of article 6.1 of the GDPR derived from having linked the registration of a

prepaid service to the NIF of the affected party, who did not intervene in the contracting of that

service, considers that there has been no illegal treatment of the NIF data of the

claimant.

It says about the individual that the treatment of the DNI number provided by the

third party applicant for the prepaid card "[...] is imposed by the provision

Unique Additional of Law 25/2007

” . And he adds that "Vodafone does not keep that data

(DNI number) related to the identity of the Complainant, but rather to the identity

(name and surname) of the Third Party. We refer to what has already been stated in the Allegation

First to avoid unnecessary repetitions.”

2. Secondly, it alleges that, in the factual assumption presented here, there were

two of the exceptions provided for in section 3 of article 17 of the GDPR:

On the one hand, the exception provided for in section b) of article 17.3: "The treatment

of the DNI number provided by the Third Party was necessary for Vodafone to

complies with a legal obligation (article 17.3 b) of the GDPR)”.

The legal obligation to process the DNI data and to keep it would be imposed by the

Sole Additional Provision and article 5, both of Law 25/2007. So, consider

that, according to the Additional Provision, "telephone operators are obliged to

to collect certain data from the applicant for a prepaid card, including "the

number corresponding to the identification document used””. and that he was bound

to keep the DNI "provided by

the contracting party of the prepaid card" by virtue of the

conservation obligation of article 5 of Law 25/2007, precept that results

applicable to the NIF data "provided by the applicant for a prepaid card" under

of the reference to that article that makes point 2 of the Additional Provision.

On the other hand, it alleges that the exception of section e) of article 17.3 of the

GDPR. It states in this regard: “Likewise, Vodafone was empowered to keep the

data provided by the Third Party in the event that in the future said data is

necessary to formulate, exercise or defend against any claim. In this sense,

the fact that Vodafone had not associated with the

Claimant's identity, but with that of the Third Party, that is, who registered the

prepaid card, which had also been marked as "fraud".”

(v) Secondarily, in the event that it is understood that the defendant has infringed

articles 6.1 and/or 17 of the GDPR and, with respect to violations of article 6.1 of the

GDPR, it is concluded that a sanction can be imposed, rejects the application of

the aggravating factors that were appreciated in the initiation agreement and requests that the

mitigations it invokes. The defendant alleges, in summary, the following:

1. Violation of article 6.1 of the GDPR, specified in the registration of a prepaid line

linked to the NIF of the claimant:

He requests that the sanction be graduated downward. He denies that the aggravating circumstances

appreciated in the initiation agreement and makes the following considerations on purpose

of every one of them:



1.1. Regarding the aggravating circumstance of article 83.2.a) of the GDPR, the duration of the

infringement taking into account the purpose of the processing operation:

“The Agency considers that we are facing a "permanent infringement", [...].

We do not agree with the consideration of this circumstance as

aggravating[...]

In the first place, [...], Law 25/2007 (Sole Additional Provision in relation to

its article 5) imposes on the operator (Vodafone) the obligation to collect and

keep "the number corresponding to the identification document used".

Secondly, article 83.2 a) of the GDPR establishes that the "duration of the

offence" will be used as an aggravating or mitigating factor "taking into account the

nature, scope or purpose of the processing operation in question,

as well as the number of interested parties affected and the level of damages

that they have suffered."

In the present case there is only one affected person (the Claimant) and no evidence has been

that damages have been generated.

Thirdly, the Judgments of the National Court of September 16,

2008 (Rec. 488/2006) and the Supreme Court of April 17, 2002 (Appeal

466/2000) cited in the Initiation Agreement are not applicable, since the

assumptions of fact and their nature are totally different. In both

rulings, which do not deal with the protection of personal data, we are before

repeated, conscious and active behavior on the part of the offenders,

elements that we did not find in the case of Vodafone.”

1.2. Regarding the aggravating circumstance of article 83.2.d) of the GDPR, 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 they have applied under articles 25 and

32”:

It refers to what was invoked in the first allegation regarding the request for the DNI to

prove the identity of the contracting party of a prepaid service. He adds that, "as regards

risks, we are not facing a case of identity theft in which the

service has been contracted "on behalf of" the Complainant, but has been

contracted by the Third Party in its own name using the DNI number of the

Claimant.”

1.3. Regarding the aggravating circumstance of article 83.2.e) of the GDPR, "Any infringement

committed by the person in charge or in charge of the treatment”:

It shows its discrepancy with the criteria of the AEPD that it has considered "background

"pertinent" the events that occurred in the following disciplinary proceedings:

PS/00193/2021, PS/00186/2020, PS/00009/2020, PS/303/2020 and PS 348/2020.”

It stresses that these procedures dealt with cases in which a third party,

posing as the claimants, contracted products on behalf of the



claimants and the latter received the corresponding invoices, which has not

happened in the alleged trial now.

1.4. On the aggravating circumstance of article 83.2.g) of the GDPR, "The categories

of the personal data affected by the infringement”:

It disagrees with the criteria of the Agency that "considers that, taking into account

the provisions of Recital 75 of the GDPR, the DNI number would be a "data

particularly sensitive insofar as a third party can supplant the

identity of a natural person with total ease, with the risks that this entails

for the privacy, honor and patrimony of the supplanted".

It justifies the non-application of the aggravating factor in that there has not been a usurpation of

identity; in which the claimant's NIF "was not exposed by Vodafone", but rather

appears published in the BOE and that it was not VODAFONE who provided the third party with the

personal data of the claimant, but rather that the third party was already in possession of that data.

We reproduce the text of his plea:

“In our opinion, there are several considerations to take into account.

First of all, Recital 75 of the GDPR refers to the fact that "the

treatment may give rise to problems of identity theft". In

In our case, unlike those cited by the Agency in the previous point, we do not

an identity theft has occurred: the Third Party has contracted in its

own name, not in the name of the Claimant. It is the Third Party who is the owner

of the prepaid card, not the Claimant.

Secondly, the DNI number (the only data affected) was not exposed by

Vodafone, but it was published – (…) – (…). (…).

In other words, it is not that Vodafone through its conduct has provided a third party with a

personal data, but that third party was already in possession of the personal data and

what it does is use it in fraud against the interested party and against the

Vodafone.”

(The underlining is ours)

It requests that the following mitigations be applied:

(Yo)

(ii)

The “absence of intentionality or negligence (article 83.2 b) of the

GDPR)”

The "cooperation with the supervisory authority by having answered the

transfer of the claim and having provided the requested information

(article 83.2 f) of the GDPR).

2. Violation of article 6.1 of the GDPR, specified in the consultation of the file of

EQUIFAX. He requests that the sanction be graduated downward. He denies the concurrence of the

aggravating factors appreciated in the initiation agreement and says in this sense:

2.1. Regarding the aggravating circumstance of article 83.2 a) of the GDPR, “The seriousness of

the infringement taking into account the purpose of the processing operation” reads:



"The Agency considers that the query to the Equifax file "represents a very

serious interference in the private sphere of the claimant", since the Claimant did not

has no relationship with Vodafone.

Without prejudice to the fact that, as seen in the Second Allegation above, the

consultation was not related to the registration of the prepaid card, article 83.2

a) of the GDPR establishes that gravity will be used as an aggravating or mitigating factor

"taking into account the nature, scope or purpose of the operation of

treatment in question, as well as the number of interested parties affected and the

level of damages they have suffered".

In the present case there is only one affected person (the Claimant) and no evidence has been

that damages have been generated."

Regarding the aggravating circumstance of article 83.2 b) of the GDPR,

2.2.

intentionality or negligence in the infringement”, it says:

"The

According to the Agency, Vodafone's lack of diligence would be "serious", since the

treatment "was carried out without having previously verified if it had the legitimacy

necessary".

As stated in the Second Allegation, Vodafone was entitled to

carry out the treatment in question under article 20.1 e) of the

LOPDGDD: the consultation was not related to the request for registration of the

prepaid card, but with a contract that supposes the financing, the payment

deferred or periodic billing.

For the rest, the ID number with which the query was made was provided

fraudulently by the Third Party, that is, it is not a consultation

done indiscriminately. Therefore, it will not be possible to appreciate a lack of

diligence, much less qualify it as serious."

23. On the aggravating circumstance of article 83.2 e) of the GDPR, "Any previous infringement

committed by the data controller", it says:

"The Agency considers that the precedents cited in the

rule on the first infringement of article 6.1 of the GDPR:

PS/00193/2021, PS/00186/2020, PS/00009/2020, PS/303/2020 and PS 348/2020" and

which, consequently, refers to what is stated in point 3 regarding the

previous violation.

2.4. On the aggravating circumstance of article 83.2 g), "The categories of personal data

personnel affected by the infringement", refers to what is alleged for this circumstance in

point 4 of the offense analyzed above.

Requests that the following extenuating circumstances apply:

Cooperation with the supervisory authority, having responded to the transfer

of the claim and having provided the requested information, article 83.2 f)

of the GDPR.

That the alleged infringement does not extend over time, article 83.2 a) of the

GDPR and 76.2 a) of the LOPDGDD.

The non-existence of benefits obtained through the infringement, article

83.2 k) of the GDPR and article 76.2 c) of the LOPDGDD.

(Yo)

(ii)

(iii)



3. Violation of article 17 of the GDPR. Requests the downward graduation of the amount of the

sanction. It rejects the application of the aggravating circumstances that were appreciated in the agreement of

start:

3.1. Regarding the aggravating circumstance of article 83.2.a) of the GDPR, “The important

seriousness of the infringement taking into account the scope of the operation of

treatment," he says:

"The Agency blames Vodafone for an "absolute ignorance of the content of the

right" of suppression, ignoring, in the opinion of this Agency, "what are the

obligations that derive for it from article 17 of the GDPR".

That being said, with all due respect, we disagree with the character

generalized subjective assessment of the Agency. As we have shown in

the Fifth Allegation, to which we refer, although the Agency ends

understanding that Vodafone has infringed article 17 of the GDPR, there are

arguments to defend that it has acted in accordance with the provisions

in article 17 of the GDPR:

a) You have not treated the DNI number illegally.

b) In any case, it was obliged by law to keep said data and, in addition,

it was necessary for the formulation, exercise or defense of

claims

3.2. Regarding the aggravating circumstance of article 83.2 b) of the GDPR, "The

intentionality or negligence of the infringement", it says:

"The Agency describes Vodafone's lack of diligence as "very serious" for not

having responded to "the deletion of the NIF data requested by the claimant despite

be obliged to do so in accordance with article 17.1 d) GDPR".

Although it is considered that the treatment of the DNI number provided by the

third party is unlawful (quod non), the obligation to

conservation imposed by Law 25/2007 which, in the opinion of this party, makes

that the infringement cannot be classified as "gross negligence".

It requests that these circumstances be applied as mitigating factors:

(Yo)

(ii)

Article 83.2.f) GDPR: "cooperation with the control authority having

responded to the transfer of the claim and provided the information

requested".

Article 83.2.k) of the GDPR and 76.2.c) LOPDGDD: the "absence of

benefits obtained through the infringement".

Finally, VODAFONE proposes as evidence the admission of the documents that

provides annexes to its allegations:

1. Screenshot "proving that the wholesaler who has signed a contract

with Vodafone is Sercom Soluciones, S.L. who, in turn, contracted with the point of

sale responsible for registering the prepaid card in question,

***ESTABLISHMENT.1”.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

19/75

2. Copy of the non-exclusive Vodafone Prepaid Wholesale Distribution contract

signed on 06/01/2019 between Sercom Soluciones, S.L., (hereinafter SERCOM) and

VODAFONE.

The twelfth clause, dedicated to "Compliance with the

applicable regulations” which stipulates: Section 12.1:

"As a consequence of the development of wholesale distribution services, the

wholesaler may access certain personal data provided that,

through you or the Retail Points of Sale to which you supply, contract

VODAFONE services. For this reason, and in accordance with the

current regulations, the WHOLESALER will be considered as the person in charge of

processing, having to formalize the standard data processing agreement that

is attached as Annex III, through which your obligations in this

subject."

Section 12.2. says:

"Likewise, the Wholesaler will transfer all obligations in terms of

protection of personal data to retail outlets and

certify that they have transferred these obligations by signing a

standard certificate attached as document IV.” (The underlining is

our)

Section 12.3. "The Wholesaler declares to know and accept the policies of VODAFONE

related to Fraud, Risk and Protection of Information included in the Annex

V of this contract, and undertakes to implement its own policies

related to these points related to the development of its activity and to transfer the

same to the Point of Sale. [....]“

Annex II to the contract, “Data collection. Wholesale distribution contract” says:

“This Annex, [...], contains the instructions regarding compliance with

the Unique Additional Provision of Law 25/2007, of October 18, of

Conservation of data related to Electronic Communications and

Public Communications Networks regarding (i) face-to-face identification and

collection of data from customers who purchase a Prepaid Card or a Pack

Prepayment prior to the sale and (ii) the information to them in the

terms described in the aforementioned Law, all in accordance with the provisions

in clause 11.2 of the Wholesale Distribution Agreement of which this Annex

bring cause.

The requirements and procedures listed below are the minimum that

The Wholesaler must comply or, failing that, the Retail Point of Sale in

compliance with the provisions of the preceding paragraph, without prejudice to the

compliance with other current procedures with the same object available

in the Commercial Portal. The Wholesaler acknowledges and accepts that they may

be modified, reduced or extended by VODAFONE in the event that it were

necessary. These updates will be timely communicated by

VODAFONE to the Wholesaler through the commercial Portal and the latter must

communicate it to the retail Points of Sale.” (The underlining is ours)

This Annex II dedicates the first stipulation to the "In-Person Identification and Collection of Customer/Buyer Data", which reads as follows:

"1. The WHOLESALER must transfer to the retail Point of Sale through the subscription of an agreement that includes obligations related in the present annex, the essential obligation to identify PRESENTIALLY the Customer /Buyer through their original identification card. * The Documentation to be presented by natural persons according to their nationality and situation is as follows: -For Spaniards: DNI or NIF. -For citizens of the European Community ID, Residence Card and Passport are accepted. -For Citizens from outside the European Community: Passport or NIE.

2. Likewise, the WHOLESALER must indicate to the retail Point of Sale the procedure to be followed to collect data and activate the credit card correct way.

The data must be collected at retail Points of Sale through the Vodafone WAS tool. It will also be possible to activate through the Web Service enabled on the WHOLESALE website, as long as it is integrated with Vodafone WAS. It will be mandatory to verify that the data provided by the Customer/Purchased and recorded by Vodafone WAS or in Web Service are correspond to the documentation provided."

copy of

contract signed between Sercom Soluciones,

3.

*** ESTABLISHMENT.1, on "04/20/2021", date after the facts.

4. Copy of the text that Sercom Soluciones, S.L. shows in its web service, which

must access the different points of sale before activating the prepaid cards of

Vodafone.

S.L.

and

5. Copy of the "General Conditions of Mobile Communications Services.

Prepaid".

It begins by indicating that "These General Conditions constitute the

Contract (hereinafter, the Contract) and are the only ones applicable to the provision of

mobile communications services of Vodafone Spain, S.A.U., [...]

Prepaid modality (card) to consumers and users [...] (hereinafter, the

Customer)."

We transcribe some of its stipulations:

"1. Object. - Vodafone will provide the Customer with the mobile telephone service and the

electronic communications services and added value that you request (in

forward, the Service).

[...]

11.- Protection of Personal Data. - According to the provisions of the Organic Law

15/1999 of Personal Data Protection (LOPD), we inform you of

that the personal data to which Vodafone has access as a result

of the provision of the Service will be incorporated into a file owned by Vodafone

and will be treated in order to provide the contracted services.

The Customer also consents to Vodafone processing their data with the following

purposes: (i) carry out general commercial actions or those adapted to your

profile, of the telecommunications and value-added services provided by

Vodafone, by companies of the Vodafone Group (www.vodafone.es) or by third parties

involved in the provision of said services, during or after

to the validity of the contract.

The aforementioned commercial actions may be carried out by any means

communication (telephone, e-mail, sms, mms…); and (ii) install and update on your

phone those applications corresponding to services of

telecommunications and value-added services provided by Vodafone, by companies

of the Vodafone Group or by third parties involved in the provision of such

services.

Likewise, the Client expressly consents that Vodafone:

a) treat your traffic and billing data, in accordance with the provisions of art. 65.3

Royal Decree 424/2005, of April 15;

b) access and process your browsing data;

c) process your location data, within the framework of the provision of services

added value implied by said location and provided that they are previously

requested by the Client and only for the time necessary to provide the

themselves;

d) transfer your personal data to companies of the Vodafone Group

(www.vodafone.es), all with the purpose of carrying out commercial actions

in the same terms indicated in section (i) of the second paragraph of this

Condition.

The Client may revoke all the consents expressed in this

Condition by addressing Vodafone with the reference "Data Protection" by

any means indicated in condition 6 of this Contract.

In relation to the data services that the Client has contracted or may

hire, we inform you that, within the framework of the provision of services

contracted, Vodafone may use tools to control the volume and

use of data to manage the operation of your network, as well as the services

contracted by the Client The Client may exercise the rights of access,

rectification, cancellation and opposition recognized in the LOPD addressing to

Vodafone by any means indicated in clause 6.”

6. Copy of the "General Conditions of Mobile Communications Services

Postpaid. Individuals".

SEVENTH: Violation of article 15 of the GDPR: Effects of the advance payment of the

sanction.

In her allegations to the opening agreement of 02/28/2022, the defendant requests that

is recognized as responsible for the infringement of article 15 of the

GDPR that was attributed to it in the aforementioned agreement and for which a possible sanction was established

administrative fine of 100,000 euros.

On 03/01/2022, VODAFONE orders a payment to the AEPD bank account

for an amount of 60,000 euros. The amount entered is the result of applying a

reduction of forty percent to the amount of the fine established for the infraction

alluded to. The defendant has made use of the two reductions provided for in sections

2 and 3 of article 85 of the LPACAP. The payment made within the period granted for

making allegations at the opening of the procedure entails the waiver of any

administrative action or appeal against the sanction and recognition of

responsibility in relation to the facts referred to in the Startup agreement.

Article 85 of the LPACAP provides in its section 3 that "the voluntary payment for the presumed responsible, at any time prior to the resolution, will imply the completion of the procedure".

Thus, the legal consequence that derives from the fact that the defendant has proceeded to the advance payment of the sanction provided for the infringement of article 15 of the GDPR is the ipso iure termination of the procedure exclusively with respect to the aforementioned infraction.

Therefore, the processing of this procedure is limited to the remaining Violations of the GDPR attributed to the claimed party: articles 6.1 and 17.

EIGHTH: Test practice.

In the procedure dated 06/27/2022, the instructor of the procedure records the opening of a test phase for a period of thirty days; that they will be practiced evidence before VODAFONE and SERCOM SOLUCIONES, S.L., (SERCOM) and the practice of the following evidentiary proceedings:

1. Consider reproduced the claim presented by the claiming party and its attached documentation, as well as the documents obtained and generated during the actions of transfer of the claim.

2. Reproduce the allegations to the agreement to start the procedure disciplinary action presented by VODAFONE and the documentation that accompanies them.

A. Test request to VODAFONE.

The respondent is required to provide the following information and documentation:

1. Copy of the Record of Treatment Activities (RAT) that was approved in September 2020.

2. Regarding the violation of article 6.1 of the GDPR derived from having processed the NIF

of the claimant linked to the registration of a prepaid line that he did not contract, the following is requested:

2.1. Copy of the form that was completed before the "***ESTABLISHMENT.1" the

person who identified himself with the claimant's NIF and requested registration of the line

prepaid.

2.2. Copy of Annex III to the "Non-exclusive Prepaid Wholesale Distribution Agreement

Vodafone" subscribed with SERCOM. Annex that deals with the treatment order

that the Distributor formalized with VODAFONE. You must provide it completed and

signed (i). Likewise, it must provide the modifications or additions to the aforementioned Annex III

that were in force in November 2020 (ii).

23. Copy of Annex IV to the "Non-exclusive Prepaid Wholesale Distribution Agreement

Vodafone" signed with SERCOM that deals with compliance by the Wholesaler of

the obligations to transfer to the retail point of sale all the obligations in

matter of protection of personal data (i) You must also provide the

certificate that he obtained from the Distributor through which he accredited that he had given



transfer of such obligations to the retail point of sale, in this case to

***ESTABLISHMENT.1,(ii).

2.4. Copy of Annex V to the non-exclusive Prepaid Wholesale Distribution Contract

Vodafone signed with SERCOM that deals with VODAFONE policies

regarding Fraud, Risk and Information Protection (i).

You must also provide: (ii) Document that VODAFONE had collected from the

Distributor in order to have documentary evidence of compliance with the obligation to inform the retail point of sale. (iii) Likewise, it must indicate if on the date November 2020 those policies (those reflected in Annex V) had been modified, reduced or extended by VODAFONE and, if so, a copy of the document in which it is collected.

2.5. Regarding Annex II to the non-exclusive Prepaid Wholesale Distribution Agreement Vodafone, subscribed with SERCOM, referring to the instructions related to the compliance with the Single Additional Provision of Law 25/2007, of October 18, Conservation of data related to Electronic Communications and Networks Public Communications to which the stipulation with which the copy is provided alludes of the contract that the Wholesaler signed with the retailer ***ESTABLISHMENT.1, it is requests:

(i) Provide a copy of the contract that the SERCOM Distributor had signed with ***ESTABLISHMENT.1, dated 11/17/2020, since the copy of the contract provided data of "04/20/2021".

(ii) Detailing the controls that VODAFONE performs with respect to the contracts entered into with retail outlets by the Distributor in order to to verify that they are adjusted to Law.

2.6. How can VODAFONE certify before this Supervisory Authority that, Indeed, the point of sale collected from the person who requested the hiring of a prepaid line your original identity document (not a photocopy), which verified your identity and who collected the client's identity data from the aforementioned document?

2.7. Regarding the document called General Conditions of the Services of Prepaid Mobile Communications that VODAFONE has contributed with its allegations to the opening agreement as annex document number 5, it is requested that you report At what point is the conditional referral delivered to the customer who hires a

prepaid line with VODAFONE through a retail point of sale.

2.8. Regarding document number 4 provided by VODAFONE, annexed to its

allegations to the start-up agreement - the screenshot of an application of

VODAFONE in which on the left appears a field with the legend "Access

customers" and below "***ESTABLISHMENT.1" and to the right "Indicate the number of

phone to activate" and "Indicates the customer data, a button with the legend "Activate" and

immediately after "vodafone activation information" that is unreadable and that

the operator has transcribed – it is requested to report the date on which such application

was operational; in particular from what date it is used with the point of sale

retailer ***ESTABLISHMENT.1.

3.Regarding the violation of article 6.1 of the GDPR derived from having made a

consult the asset solvency file ASNEF using as criteria of

search for the NIF of the claimant, the following is required:

3.1. Documentary evidence that, as stated in his allegations to the

startup agreement, you received an online request to purchase a product or service that

involved financing or periodic billing in which the applicant identified herself with



the NIF of the claimant. You must provide (i) the documents that prove the request

received and (ii) the documentation that was then collected from the applicant for the contract to

in order to verify your identity.

3.2. Documentary evidence that the person who requested to hire a service

postpaid that led him to make a query to the ASNEF solvency file using

as search criteria, the NIF of the claimant was informed of this treatment,

prior to the consultation, in compliance with the provisions of article 13 of the

GDPR.

4. Regarding the violation of article 17 of the GDPR attributed to VODAFONE, it is

requests:

4.1. That he explain the reasons why he did not proceed "without undue delay" to delete

the NIF data of the claimant under article 17.1.d) RGPD since the

entity was fully aware that the claimant's data had been

linked to fraudulent recruitment. In this regard, we refer to the emails

exchanged with the claimant from which it turns out that on the date

02/03/2021, when the police report was already in the possession of VODAFONE

filed by the claimant and various documents submitted by her, acknowledged that

it was a fraud, despite which until 05/27/2021, as stated, no

deleted the claimant's data from its systems.

B. Evidence request to SERCOM related to the “Distribution

Prepaid Wholesaler. Not exclusive to Vodafone”, which signed with that operator the

06/01/2019.

The electronic notification was made available to the recipient on 06/27/2022

being rejected on 06/08/2022.

NINTH: VODAFONE's response to the tests carried out.

On 07/21/2022, the AEPD received the respondent's response to the evidence

practiced.

1. At the request that you provide a copy of the RAT that was approved in

September 2020, he submits a document from which he comments that it is "current in

November 2020” and “which applies to both franchises and wholesalers”.

The document, identified with number 1, is headed "Details of the activity

of processing” (Processing Activity Details). The information relates exclusively to

on “Distribution–Franchise Distributors”. In the section "Description of the

treatment”, mentions the “management of franchise stores” and says that the

treatment is the same as in VODAFONE's own stores with two

differences: “but with two different ERP in the front.”.

VODAFONE is not clearly identified as the data controller. HE

uses the reference "1.0" in the description of the treatment carried out by the

person in charge of treatment and the purposes of the treatment. On the legal basis

of the treatment says that “individuals have consented to the treatment

of your personal data for one or more purposes.”



2. In relation to the violation of article 6.1 of the GDPR derived from the registration of a line

prepayment linked to the NIF of the claimant:

2.1. It is requested that you provide a copy of the form that the customer who contracted the line

prepayment completed in the ***ESTABLISHMENT.1. This request had its reason

be that, according to the "Retail Distribution Agreement" between SERCOM and

***ESTABLISHMENT.1, "If the operator requires it, the point of sale

You will need to print the form in duplicate, get the customer's signature, give them a

copy and keep the other for collection by Sercom staff.”

(stipulation 4.3)

VODAFONE responds by sending another document other than the one requested: it provides a

screenshot with the information that was incorporated into the computer application of

SERCOM, a document that he had already provided.

2.2. Taking into account that section 12.2 of the Wholesale Distribution contract

concluded between VODAFONE and SERCOM that provided the AEPD with the allegations to the

initiation agreement established that "the Wholesaler will transfer all obligations

regarding the protection of personal data at points of sale

Retailers and will certify having transferred these obligations by signing

a standard certificate that is attached as document IV.", it was requested to that

operator that provided the aforementioned annex IV and "the certificate that it obtained from the Distributor

by means of which he accredited that he had transferred such obligations to the point

of Retail sale, in this case to ***ESTABILIENTO.1".

VODAFONE responds by twice providing a document that certifies nothing.

The document sent is a form (identified as annex IV) in which,

In addition to not having completed the certifying data (it should be

SERCOM), since the spaces for the NIF, name, address and details of the

representative are empty, there is no SERCOM stamp or signature. Figure the seal of

VODAFONE stamped twice and a signature with no indication of who it belongs to. No

There is no mention of SERCOM in the document.

23. VODAFONE was requested to provide a copy of annex V to the Distribution Agreement

Prepaid Wholesaler subscribed with SERCOM and the copy of the document that VODAFONE

would have been collected from the distributor in order to have documentary evidence of the

compliance with the obligation to inform the retail point of sale.

VODAFONE provides the aforementioned annex V, which is headed "Anti-corruption policy,

economic sanctions and corporate security" but has not submitted any documents

certifying that SERCOM informed the point of sale. It has limited itself to providing two

annexes to annex V: A. “Individual confidentiality agreement. Data and information

owned by Vodafone Spain, S.A.U.” and B. “Safety rules and procedures.

Summary of general safety regulations". In both documents (A and B) do not appear

Once the identifying data of the declarant has been filled in, that is, we are facing a

form in which no one is identified as the author of the statement contained in them

collect. There is no seal or signature of SERCOM. The stamp of

VODAFONE. Also a rubric to which it is unknown who it belongs to.



2.4. Annex II to the Wholesale Distribution Contract signed with SERCOM, versa

on the instructions regarding compliance with the Sole Additional Provision of

Law 25/2007.

VODAFONE was asked to provide (i) a copy of the contract that the distributor

SERCOM had subscribed with ***ESTABLECIMIENTO.1, on 11/17/2020, whenever

that the copy of the contract provided dates from "04/20/2021", and (ii) that it detail which

were the controls that VODAFONE carries out regarding the contracts entered into by the

distributor, SERCOM, with the retail outlets in order to verify that they are

adjusted to law.

Regarding the controls, VODAFONE has responded:

"[...] in relation to the controls that Vodafone performs regarding the contracts

entered into between wholesalers and retailers, they are detailed in the

following clauses:

Clause 11.1 of the contract between Vodafone and SERCOM (Document 2 of the written

of Allegations to the Commencement Agreement): "In order to guarantee the quality

of the VODAFONE services associated with the Products and the prestige of its

brand, the traceability of the activated Products and avoid Fraud and/or Deception

Commercial, the WHOLESALER must provide VODAFONE daily through

Vodafone WAS a report on all Retail Points of Sale with

who works as well as the type of product supplied to them by

of the WHOLESALER including the following information of each Point of Sale

Retail:

• On each Retail Point of Sale: Detail of the commercial name, CIF,

company name, address, telephone number, town, postal code and sector of

activity,

• On the products sold by the WHOLESALER at each Point of Sale

Retailer: Number of products sold by product type, MSISDN in your

case and date of purchase of the product by the Retail Point of Sale. Yeah

the date of information to VODAFONE of the products sold by the

WHOLESALE to retail point of sale is after the activation date

of the MSISDN by the retailer or, if the activation of the products is carried out

with a NIF/CIF of a retail Point of Sale other than the one informed by

of the WHOLESALER, the action of the WHOLESALER may be considered Deception

Commercial.

[...]".

Clause 9 of the treatment contract (Document 3): "The

Processor will ensure that any Subprocessor

Treatment allows Vodafone, its customers (including subcontractors,

auditors or other agents of Vodafone and their respective clients) and/or the

Privacy Authorities (each an "Audit Party") to access

to its computer systems and other information systems, records,

documents and agreements that are reasonably required by the Auditing Party, to

verify that the Treatment Manager and/or his Sub-Managers are

complying with its obligations under this Agreement (or

any subsequent sub-Processing contract) or any Sub-Processing Legislation

Applicable Privacy [...]".



In addition, as noted in section iii. above, through Annex IV

the wholesaler certifies that the obligations have been transferred to the points of sale

applicable in terms of data protection."

In short, the controls consist of:

1. In the obligations established in clause 11.1 of the contract of

Distribution, according to which the distributor undertakes to inform the operator of the

identity of the points of sale with which you enter into contracts and the products

supplied. Extremes that do not allow in any case to control if the points of

sale follow the card purchaser identification protocol. It's more,

It is not even mentioned among the obligations assumed by the SERCOM distributor the

to provide VODAFONE with a copy of the contractual documents it signs with

the points of sale. Stipulation 9 of the treatment order contract,

provision that does not contemplate actions to verify the identity of the

contracting of prepaid cards.

2. Through a document issued by the wholesaler certifies that it has transferred to the

points of sale the applicable obligations regarding data protection according to

the model that appears as annex IV of the distribution contract. However, in the

certificate provided, as previously stated, nothing is accredited since it

provided by VODAFONE is not a certificate issued by the SERCOM distributor but rather

an unfilled form bearing the VODAFONE stamps.

2.5. To the question asked about how VODAFONE could accredit before the AEPD

that the point of sale collected from the person who requested the contracting of the line

prepaid your original identity document (not a photocopy); that point of sale

verified his identity and that he collected from the aforementioned document the identity data of the

client, the defendant does not prove anything and merely responds referring again to the

contract entered into with the point of sale (document 6). Says the following:

"As indicated in the pleadings to the Commencement Agreement, SERCOM is

forced to transfer to the point of sale the "essential obligation to identify

IN PRESENTIALITY to the Client/Buyer through his identification card

original". In addition, it is specified that "the documentation to be presented by the

individuals" consists of the "DNI or NIF" or the "Passport or NIE"

(Document 2 of the brief of Allegations to the Commencement Agreement).

In turn, this obligation was transferred to the point of sale

(***ESTABLISHMENT.1), as evidenced by Document 6 provided with

this writing:".

The mentioned document 6 corresponds to the contract between SERCOM and the point of

retail ***ESTABLISHMENT.1.

2.6. VODAFONE provides a copy of the retail distribution contract for

telephony signed between SERCOM and ***ESTABLECIMIENTO.1, (document number 6).

The only reference that exists in it to the obligations of which it supposedly

SERCOM should inform you regarding the identification of the acquirers

of the cards, is this, in which, as can be verified, the client is not required to

Provide the original identification document. The General Conditions of the contract,

Stipulation 4, "Requirements for the collection of SIM/PACK customer data:", says:

“4.1. In compliance with the provisions of the Sole Additional Provision of the

Law 25/2007 of October 18, on the Conservation of Data Related to

Electronic Communications and Public Communications Networks, the

Authorized Point of Sale when selling a SIM/PACK must comply with the

following obligations

to. Keep a book-registry in which the identity of the clients that

acquire a smart card with said payment method.

b. Prior information to customers about the existence and content of the record,

of its availability in the terms expressed in the number

following and of the rights included in article 38.6 of Law 32/2003.

c. The identification will be made by means of a document accrediting the

personality, recording in the registry book the name, surnames and

nationality of the buyer, as well as the number corresponding to the document

identification used and the nature or name of said document. In it

case of legal persons, [...]

d. In cases where the operator requires it, collect and send the

documentation signed by the client to the place indicated by Sercom. [...] (He

underlined is ours)

Stipulation 11. “Protection of customer personal data.

"The point of sale will comply with the provisions of Law 25/2007, of 18

October; Regarding the conservation of data collected from users,

being, therefore, their sole responsibility for compliance or not with the

current legislation on data protection. The Point of Sale acknowledges

expressly comply with all the requirements demanded by Law 15/1999 of

Data Protection."

3.Regarding the infringement of article 6.1 of the GDPR derived from consulting the file

of financial solvency ASNEF using the NIF of the claimant, it was required to

VODAFONE that accredits two extremes:

1. The alleged receipt of an online request made by someone who identified themselves with

the NIF of the claimant to contract a product or service that implied

Financing or periodic billing. In this regard, these documents were requested:

that certify the receipt of the application for the product to which it alludes and those that are

collected from the applicant in order to verify their identity.

2. That the person who requested to contract an online service was informed, on a

prior to the treatment (the consultation), as required by article 13 of the GDPR.

The defendant responds to the request for evidence saying:

“Vodafone has not been able to locate the request in question. However, as

As noted in the pleadings to the Commencement Agreement, the consultation with the

ASNEF file was not linked to the registration of the prepaid card, in the

to the extent that the registration of prepaid cards does not imply a scoring process or the

consult delinquency files.” (The underlining is ours)

Regarding the second request, it says:

"We refer to what was stated in the answer to the previous question."

4.Regarding the infringement of article 17 of the GDPR, VODAFONE was asked to explain the reasons why it did not proceed "without undue delay" to delete the data of the NIF of the claimant under article 17.1.d) GDPR from the moment in which that he learned that he had been linked to a fraudulent contract, while the emails exchanged with the claimant evidenced "that on the date 02/03/2021, when the police report was already in the possession of VODAFONE filed by the claimant and various documents submitted by her, acknowledged that it was a fraud, despite which until 05/27/2021, as stated, no deleted the claimant's data from its systems."

VODAFONE responded by reiterating what was alleged about this infringement of the GDPR in its pleadings to the initiation agreement.

TENTH: Resolution proposal.

The resolution proposal, signed and notified on 10/10/2022, was formulated in the following terms:

<<1. That the Director of the Spanish Data Protection Agency sanction to VODAFONE ESPAÑA, S.A.U., with NIF A80907397, for a violation of article 6.1. of the GDPR, typified in article 83.5.a) of the GDPR, materialized in having given registration of a prepaid line associated with the NIF of the claimant, with a fine of 70,000 € (seventy thousand euros).

2. That the Director of the Spanish Agency for Data Protection sanctions VODAFONE ESPAÑA, S.A.U., with NIF A80907397, for a violation of article 6.1. of the GDPR, typified in article 83.5.a) of the GDPR, specified in having consulted a credit information file using the NIF of the claimant as criteria without be legitimized for this treatment, with a fine of €70,000 (seventy thousand euros).

3. That the Director of the Spanish Agency for Data Protection sanctions

VODAFONE ESPAÑA, S.A.U., with NIF A80907397, for a violation of article 17

of the GDPR, typified in article 83.5.b) of the GDPR, with a fine of €100.00 (one hundred thousand

euro).>>

The certificate issued by the FNMT certifying that the

Notification was accepted by the defendant on 10/17/2022.

Thus, being ten days the period granted to formulate allegations to the

proposed resolution in accordance with article 73.1 of the LPACAP, the aforementioned term

would end on 10/31/2022.

ELEVENTH: On 10/18/2022, a letter from VODAFONE was received at the AEPD

in which you request that the term granted be extended, by the maximum legally permitted

to formulate allegations to the proposed resolution.



The AEPD responds on 10/19/2022 denying the requested extension. The writing of

response is notified to the defendant on 10/19/2022.

To the reasons given by VODAFONE to justify its request for extension -which

“the term initially granted [...] does not allow the proper formulation of the appropriate

allegations and gather the necessary evidence” due to “the complexity of the

procedure and the amount of the sanction that could correspond"- it was answered that

no document was involved in the procedure that was unknown to the

claimed, therefore, on the one hand, he had been delivered a copy of the file

before the processing of allegations to the initiation agreement and, on the other, the only evidence that

were carried out with the obtaining of documentation, they had been carried out before the VODAFONE since SERCOM did not even accept the notification. HE added that the defendant had had the opportunity to provide evidence in the proceedings of allegations to the initiation agreement and in the test phase and that the proposal for resolution maintained the legal qualification of the facts that was made in the agreement of beginning, limiting itself, in essence, to rebutting the arguments that the defendant had used in his defense in his allegations to the opening agreement.

TWELFTH: VODAFONE does not make any arguments regarding the proposed resolution.

As of 11/03/2022, three days after the end of the period granted for make allegations to the proposed resolution, have not had input into the Record of this Agency the allegations of VODAFONE.

Pursuant to article 73.1 of the LPACAP, the term to make allegations is ten business days, which must be counted from the day following the acceptance of the notification. Thus, having accepted VODAFONE the notification of the proposal resolution on 10/17/2022, the claim period ended on 10/31/2022.

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

PROVEN FACTS

FIRST: The claimant, A.A.A., holder of NIF ***NIF.1, denounces that VODAFONE, entity of which you are not a customer, has registered a telephone line associated with your NIF prepaid without your knowledge or consent; have consulted the system EQUIFAX credit information using your NIF as search criteria and not has addressed the rights of access and deletion that it exercised before the operator.

SECOND: VODAFONE processed the claimant's NIF data linked to the registration of a prepaid telephone line, number (...), dated November 17, 2020. They work in the file, provided by VODAFONE with its response to the request

information from the Data Inspection Sub-directorate, various screenshots

of their computer systems (annex documents 3 and 4) in which the

customer account ID ***ID.1, corresponding to the telephone number and the date

mentioned, and linked to the name of B.B.B. and the NIF of the claimant, ***NIF.1. He

NIF data is registered in the "(...)" in the "Info. contact".



THIRD: VODAFONE declares that it was entitled to process the NIF data of

the claimant who was provided by the third party who intervened in the contracting and that the basis

legal processing is article 6.1.c) of the GDPR in connection with the Provision

Unique Additional of Law 25/2007. The defendant has stated:

"Vodafone is obliged by Law 25/2007 to treat the "number corresponding to the

identification document used" by the buyer of the prepaid card; question

Another difference is that said number turns out to be wrong or has been used by a

fraud by a third party, but this may not imply, in any case, a violation of the

article 6.1 of the GDPR."

FOURTH: VODAFONE acknowledges in its allegations to the initiation agreement (allegation

third) that the NIF data of the claimant who was subject to treatment linked to

the prepaid line does not belong to the purchaser of the card. The entity has said:

"[...] there may be cases, such as this one, in which Vodafone processes data

staff that does not belong to the applicant for the prepaid card, but to a third party (the

claimant). This is what has happened in this case: it is evidence and we do not deny it."

FIFTH: VODAFONE states that the third party that contracted with it and identified himself

with the NIF of the claimant "satisfactorily passed the security policies" of the company "because to carry out the registration of a prepaid line the exhibition is required of an official identification document before the agents of the physical stores". Ha declared that he did not know of the existence of this fraud until he was notified by the claimant and that at that moment "a procedure is initiated to verify the facts and fix the situation." VODAFONE received the copy of the complaint that the claimant filed with the police on 12/21/2020.

SIXTH: The Wholesale Distribution contract signed between VODAFONE and SERCOM, clause 12.2, says that SERCOM "will notify all obligations regarding protection of personal data to retail outlets and certify that they have transferred these obligations by signing a standard certificate attached as document IV."

VODAFONE in the test phase is required to provide the issued certificate by SERCOM under the aforementioned stipulation. In response, he contributes a document -form annex IV- in which there is no mention of SERCOM. In the document does not include the data of the certifier (it should be SERCOM). The spaces for the NIF, name, address of the certifier and the details of your representative are empty; there is no seal or signature of SERCOM. There's a VODAFONE stamp stamped twice and a signature with no indication of who belongs.

SEVENTH: Annex II to the contract between SERCOM and VODAFONE, "Data collection. Wholesale Distribution Agreement", contains the instructions relating to the compliance with the Sole Additional Provision of Law 25/2007, regarding (i) the face-to-face identification and data collection of customers who purchase a Card Prepaid or a Prepaid Pack prior to the sale and (ii) the information to the themselves in the terms described in the aforementioned Law, all in accordance with the

provided in clause 11.2 of the Wholesale Distribution Contract of which the Annex bring cause.

Its first stipulation, "In-person Identification and Data Collection of the Client/Buyer", says:

"1. The WHOLESALER must transfer to the retail Point of Sale through the subscription of an agreement that includes obligations related in the present annex, the essential obligation to identify PRESENTIALLY the Customer /Buyer through their original identification card. * The Documentation to be presented by natural persons according to their nationality and situation is as follows: -For Spaniards: DNI or NIF. -For citizens of the European Community ID, Residence Card and Passport are accepted. -For Citizens from outside the European Community: Passport or NIE. [...]."

The contract for the retail distribution of telephony products signed between SERCOM and *** ESTABLISHMENT.1, (document number 6 of those provided in the phase of proof) does not include the obligation for the client to show the original document. His Stipulation 4, "Requirements for the collection of SIM/PACK customer data:", says:

"1. In compliance with the provisions of the Sole Additional Provision of the Law 25/2007 [...], the Authorized Point of Sale when selling a SIM/PACK must comply with the following obligations

[..]"

c. The identification will be made by means of a document accrediting the

personality, recording in the registry book the name, surnames and

nationality of the buyer, as well as the number corresponding to the document

identification used and the nature or name of said document. In it

case of legal persons, [..]"

EIGHTH: VODAFONE in the test phase is requested to detail which are the

controls that it performs regarding the contracts entered into by the distributor, SERCOM,

with retail outlets in order to verify that they are in accordance with the law.

From his answer -which is reproduced in detail in the eighth Antecedent- the controls

its about:

1. A document issued by the wholesale distributor certifying that it has

transferred to the points of sale the applicable obligations in terms of protection

of data, annex IV of the distribution contract. We refer to the Proven Fact

SIXTH.

2. The obligations established in clause 11.1 of the Distribution contract, to

according to which the Distributor undertakes to inform the operator of the identity of

the points of sale with which it enters into contracts and the products supplied, and the

stipulation 9 of the treatment contract between SERCOM and VODAFONE.

NINTH: The defendant in the trial phase is requested to provide a copy of the RAT. He

document that it provides (number 1 of those sent in the test phase) versa,

exclusively, on the activity of the Distributors-Franchisees and does not specify if

the processing of personal data to which you are referring has to do with the one

made with the sale of prepaid products or other types of products. As base

legal treatment says that "people have given their consent to the

processing of your personal data for one or more purposes".

TENTH: There is an EQUIFAX document in the file with the date

"11/12/2020" that includes the result of the search carried out on that date in the

ASNEF file using the claimant's NIF as criteria. In the section of

document "History of queries" a query made by

"Vodafone One, S.A.U." on 09/15/2020, at 18:40.27.8 hours.

ELEVENTH: VODAFONE acknowledges in its allegations to the start-up agreement that

consulted the ASNEF file using the claimant's NIF as an identifier;

declares that the query was linked to "an online request" that he had received and

that "the product in question about which Equifax was inquired was a

product related to financing, deferred payment or periodic invoicing, so

falls within the scope of application of article 20.1.e) of the LOPDGDD".

TWELFTH: VODAFONE in the test phase is requested to accredit

documentary proof that you received an online application to hire a product or service

involving financing or periodic billing by a person who identified himself

with the NIF of the claimant. In particular, they were asked to provide (i) the documents that

prove the request received and (ii) the documentation that was then collected from the

contract applicant in order to verify their identity.

The defendant responds: "Vodafone has not been able to locate the request in question" (The

underlined is ours)

THIRTEENTH: There is in the file the following documentation that accredits

that the claimant exercised the right of access and the terms of the response of

VODAFONE, both to the exercise of the right by the claimant and to the petition

information that the AEPD Inspection Sub-directorate addressed to him on the matter:

1. An email that the claimant sends on 12/19/2020 to

derechosprotecciondatos@vodafone.es

account

(***USUARIO.1@gmail.com) in which you request access to your data and with the

Provide a copy of your ID.

from

his

2. An email from VODAFONE to the claimant, dated 12/21/2020, at 7:20 p.m.

hours, in which he acknowledges receipt of the petition and replies that, in accordance

with article 15 of the GDPR, "We regret to inform you that there is no

legitimized to obtain the right of access with respect to the data

personal information (National Identity Document) that appear in the system of

VODAFONE ESPAÑA since you do not register in it as the owner of the

data required. We remind you that, if you wish, you can exercise your rights

deletion, access, limitation, rectification and portability by sending

a written communication, accompanied by a copy of your ID or document

equivalent identification, to the address [...]" (The underlining is ours)

3. An email that the claimant sends to VODAFONE on 12/21/2020, at 20:21

hours, with this text: "A complaint filed with the national police is attached

due to a usurpation of my identity, for which I am requesting the



access to personal data that may appear related to my ID or

name, since you have consulted my data on 09/15/2020 18:40:27 in

an Equifax file illegitimately since I do not have any contract or

relationship with you." Attached to it, in addition to the DNI and the letter requesting the

access, police report.

4. An email from VODAFONE dated 12/29/2020 acknowledging receipt of the request

of access of December 21 and responds in the same terms as in its

previous answer (point 2).

5. A screenshot of the VODAFONE systems (document 2 attached to the

response to the request for information from the Sub-directorate of Inspection) in

whose image is seen, in the "Calling information" tab the ID ***ID.1 (to which

the NIF of the claimant and the name and surname of the third party are linked) and

below the tab corresponding to "request 10915XXXX". in it is

registered as "Title" "Fraud", as "Type" "Fraud" and as "Code of

opening" "Fraud". The text of the request is transcribed below

formulated by the claimant, in which she identifies herself by her name, surname, NIF

and domicile; states that you wish to exercise the right of access; asks you

provide "information about their personal data, contracts, etc. that may

appear in your company." and indicates that you provide a copy of your ID.

6.VODAFONE responds to the information request of the Sub-directorate of

Inspection of the AEPD that the claimant exercised before her the right of access

to your data on December 19, 2020 and that he responded on December 21,

2020 informing her "that she is not legitimized to obtain the right

of access with respect to personal data (National Document of

Identity) that appears in the system of my [the claimed] since Mrs. [the

claimant] is not registered as the owner of the required data." "This is

because the data of Ms. [the claimant] were related to a

third party that used the data of the Interested Party fraudulently. In this

Of course, the only personal data of the claimant that is related to this

fraud is the DNI, which is why in the evidence provided by the

systems of my represented appears information from a third party "B.B.B.", with the

DNI of the claimant ***NIF.1.” (The underlining is ours)

FOURTEENTH: There is in the file this documentation that certifies that the

The claimant exercised the right of deletion and the response received from VODAFONE:

1. An email that the claimant sends to VODAFONE on 01/24/2021,

derechosprotecciondatos@vodafone.es, with this text:

“This email is sent to request the deletion of my data from your databases.

data, since they do not provide me with the information related to my ID, and I do not

should have none of my data as I have no relationship with

Vodafone.” (The underlining is ours)

The claimant attached to her email her signed request for deletion of data; his

DNI and "copy of the expansion of the complaint in which the

national police the information that they give me together with that of other companies. [...]”



2. An email from VODAFONE to the claimant, dated 01/26/2021, in which

responds: "[...] In view of your request, in which you exercise the right of

deletion of your personal data in accordance with article 17 of the

Regulation (EU) 2016/679 [...] We regret to inform you that this entity does not

can generate the deletion of the requested data since they are

necessary to provide the service to the prepaid line ***TELEPHONE.1,

we understand the purpose of your request, however, and in case of not

recognize the product we could generate a rectification of data so that the

service is in your name and you can make use of it; we emphasize that the

prepaid products cannot be deactivated, otherwise we can wait

until the card expires (Approximately estimated expiration date is June

of 2021 if no recharges are generated), after that you could request your

right of erasure." (The underlining is ours)

3. An email that the claimant addresses to VODAFONE on 02/01/2021 with this text:

"[...] They tell me from the Vodafone Spain facebook channel that they opened the

request number 10915XXXX to the fraud department, where they notify that

Indeed there is an error and it is solved. Can you confirm the

deletion of my data? [...] "

4. VODAFONE reply email of 02/03/2021 in which it says that "[...]

In response to your email, we must inform you that the line ***TELEPHONE.1

corresponding to the file registered with its National Document number of

Identity was expired by our fraud area in order to avoid

any type of use, however, it still registers in our system and

It will only be disconnected until June 2021, which makes it impossible for

Your data is deleted from our system.

However, the data protection department generates a statement

alerting all our areas to omit any type of management on

the fraudulent file, attached to it we generate the opposition to the treatment and use of the

data for commercial purposes.

Finally, we make the clarification that your request (Deletion of data)

It can only be attended to until the previously stated date (June

2021), therefore it is necessary that you send us this request at the end of the month

exposed. [...]" (emphasis added)

FIFTEENTH: VODAFONE has invoked these reasons to explain why it did not

proceeded to suppress the NIF of the claimant "without undue delay", in accordance with

Article 17.1.d) of the GDPR, after learning that he was linked to a

fraudulent recruitment:

- "[...], Vodafone does not keep the DNI number related to the identity of the

Claimant, but with the identity (name and surname) of the third party who gave

register the prepaid card."

- That two of the exceptions of article 17.3 of the GDPR concur:

Section b), "The treatment of the DNI number provided by the third party was

necessary for Vodafone to comply with a legal obligation", in connection

with the Sole Additional Provision and article 5 of Law 25/2007.

Section e): "The treatment of the DNI number provided by the third party was

necessary for the formulation, exercise or defense of claims".



SIXTEENTH: VODAFONE states in its response to the request for information

of the Sub-Directorate of Inspection that dealt with the right to suppress the

claimant and deleted their NIF from their systems on 05/27/2021.

SEVENTEENTH: Document number 4 of those that VODAFONE provided to the

Sub-directorate of Inspection with its response to the information request, includes two

screenshots that prove that on 01/26/2021 they existed in the systems of the

operator claimed records mentioning the fraudulent nature of the

prepaid line linked to the NIF of the claimant. In the document, the “(...)” incorporates the

following information: In the "Customer registration" tab, it appears with the "Order number

V” the reference ***REFERENCE.1; as "Title" "Prepaid Installation With..." and as

"F. Opening” “11/17/2020”. In the lower box, "Requests, claims,

breakdowns", several claims are registered, including one dated 01/26/2021 with

this information: As "Type", there is "Fraud"; as “Code”, “possible fraud” and

as “Subcode”, “Impersonation”.

FUNDAMENTALS OF LAW

Yo

Competition of the AEPD

By virtue of the powers that article 58.2 of Regulation (EU) 2016/679, of the

European Parliament and of the Council, of April 27, 2016, regarding the protection of

natural persons with regard to the processing of their personal data and the

free movement of these data and repealing Directive 95/46/CE (GDPR),

recognizes each control authority and as established in articles 47 and 48 of

Organic Law 3/2018, of December 5, on the protection of personal data and

guarantees of digital rights (LOPDGDD), the Director of the Spanish Agency

of Data Protection is competent to initiate and resolve this procedure.

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

Procedure that is substantiated before the AEPD

Title VIII of the LOPDGDD is headed "Procedure in case of possible

violation of data protection regulations" (articles 63 to 69) Article 63.2

provides that "The procedures processed by the Spanish Agency for the Protection

of Data will be governed by the provisions of Regulation (EU) 2016/679, in this

organic law, by the regulatory provisions issued in its development and, in

as long as they do not contradict them, on a subsidiary basis, by the general rules on

administrative procedures."



In accordance with articles 63.1 and 64.1 and 2 of the LOPDGDD, the procedures that are

processed by the AEPD are two: Those in which "an affected person claims that he has not

your request to exercise the rights recognized in articles 15 has been addressed

to 22 of Regulation (EU) 2016/679" and those that "have as their object the

determination of the possible existence of a violation of the provisions of the

Regulation (EU) 2016/679 and in this organic law". Article 64.1 of the

LOPDGDD refers to the first of the procedures indicated when seeing

"exclusively" on "the lack of attention to a request to exercise the

rights established in articles 15 to 22 of Regulation (EU) 2016/679."

If the affected party does not request the AEPD "exclusively" the protection of the rights that

recognized in articles 15 to 22 of the GDPR, but simultaneously

file a claim for an alleged infringement of the protection regulations

of personal data, it is up to the AEPD to determine if both

claims will be substantiated or not in the same procedure.

As the AEPD indicated in the agreement to open this procedure, in the event raised here, in which the claimant requests protection of the rights that she has recognized in articles 15 and 17 of the GDPR and, simultaneously, denounces the infringement of provisions of the GDPR, it was deemed appropriate to process both claims through the disciplinary procedure. In the decision adopted assessed the seriousness of the conduct of the defendant who, under the appearance of having attended to the rights whose protection was claimed, acted ignoring radically its content. Also, the large volume of personal data that the claimed treats in the development of its business activity because we are before the first mobile telecommunications operator in the national market by number Of customers.

II

Article 85 of the LPACAP and violation of article 15 of the GDPR.

Article 85 of the LPACAP provides:

"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 responsible 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."

In the seventh Antecedent of this resolution it is stated that VODAFONE proceeded in

date 03/01/2022 to the advance payment of the sanction established in the opening agreement

for the violation of article 15 of the GDPR with a reduction of forty percent.

Pursuant to article 85.3. of the LPACAP the anticipated payment of the sanction foreseen

caused the termination of the disciplinary procedure with respect to said infraction.

IV.

applicable provisions

The RGPD deals in its article 5 with the principles that govern the treatment of personal data.

personal data, precept that provides:

"1. Personal data will be:

a) Treated in a lawful, loyal and transparent manner with the interested party (<<legality, loyalty and

transparency>>)

b) [...] ("purpose limitation");

c) [...] ("data minimization");

d) accurate and, if necessary, up-to-date; all measures will be taken

Reasonable reasons for the erasure or rectification without delay of the personal data

are inaccurate with respect to the purposes for which they are processed ("accuracy");

e) [...] ("retention period limitation");

f) processed in such a way as to guarantee adequate data security

personal data, including protection against unauthorized or unlawful processing and against

its loss, destruction or accidental damage, through the application of technical measures

or organizational ("integrity and confidentiality").

2. The controller will be responsible for compliance with the provisions

in section 1 and able to demonstrate it (<<proactive responsibility>>)”

Article 6 of the GDPR under the heading "Legacy of the treatment" specifies in its section

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

"1. Processing will only be lawful if it meets at least one of the following

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 to the treatment

carried out by public authorities in the exercise of their functions."

For its part, the LOPDGDD establishes in article 20, under the heading "Systems of

credit information":

"1. Unless proven otherwise, the processing of personal data will be presumed lawful.

related to the breach of monetary, financial or credit obligations by

common credit information systems when the following are met

requirements:

to) [...]

b) [...]

c) [...]

d) [...]

e) That the data referring to a specific debtor can only be

consulted when the person consulting the system maintained a contractual relationship

with the affected party that implies the payment of a pecuniary amount or this would have

requested the conclusion of a contract that involves financing, deferred payment or

periodic billing, as happens, among other cases, in those provided for in the

legislation on consumer credit contracts and real estate credit contracts.

When the right to limitation of processing has been exercised before the system

of the data challenging its accuracy in accordance with the provisions of article 18.1.a) of the

Regulation (EU) 2016/679, the system will inform those who could consult it with

accordance with the previous paragraph about the mere existence of said circumstance, without

provide the specific data with respect to which the right had been exercised, in

both are resolved on the request of the affected party.

f) That, in the event that the request for the conclusion of the contract is denied, or it

will not be held, as a result of the consultation carried out, whoever has

Once the system has been consulted, inform the affected party of the result of said consultation."

Chapter III of the GDPR, "Rights of the interested parties", refers, among others, to the

right to delete data. Article 17 of the GDPR provides:

"Right to erasure ("the right to be forgotten")

"1. The interested party shall have the right to obtain without undue delay from the person responsible for the

treatment the deletion of personal data that concerns you, which will be

obliged to delete without undue delay the personal data when any

of the following circumstances:

a) the personal data is no longer necessary in relation to the purposes for which it was

were collected or otherwise processed;

b) the interested party withdraws the consent on which the treatment is based in accordance

with Article 6(1)(a) or Article 9(2)(a) and this is not

based on another legal basis;

c) the interested party opposes the processing in accordance with article 21, paragraph 1, and does not

other legitimate reasons for the treatment prevail, or the interested party opposes the

treatment according to article 21, paragraph 2;

d) the personal data have been unlawfully processed;

e) personal data must be deleted to comply with a legal obligation
established in the law of the Union or of the Member States that applies to the
responsible for the treatment;
f) the personal data have been obtained in relation to the offer of services of the
information society referred to in article 8, paragraph 1.
2. When you have made the personal data public and are obliged, by virtue of the
provided in section 1, to delete said data, the person responsible for the treatment,
taking into account the technology available and the cost of its application, it will adopt
reasonable measures, including technical measures, with a view to informing
responsible who are processing the personal data of the request of the interested party
deletion of any link to such personal data, or any copy or replica of
the same.
3. Sections 1 and 2 will not apply when the treatment is necessary:
a) to exercise the right to freedom of expression and information;
b) for compliance with a legal obligation that requires data processing
imposed by the law of the Union or of the Member States that applies to the
responsible for the treatment, or for the fulfillment of a mission carried out in the interest
public or in the exercise of public powers conferred on the person responsible;
c) for reasons of public interest in the field of public health in accordance with
Article 9, paragraph 2, letters h) and i), and paragraph 3;
d) for archiving purposes in the public interest, scientific or historical research purposes or
statistical purposes, in accordance with Article 89(1), to the extent that
the right indicated in paragraph 1 could make it impossible or hinder
seriously impair the achievement of the objectives of such treatment, or
e) for the formulation, exercise or defense of claims." (The underlining is

our)

V

Violation of article 6.1. of the GDPR: Treatment of the NIF of the linked claimant

when registering a prepaid line.

1. In the initial agreement, VODAFONE was attributed a violation of article 6.1. of the

GDPR derived from having processed the NIF of the claimant linked to a line

prepaid that she did not contract, since the treatment of that personal data does not

it was based on none of the causes of legality that the precept establishes.

In its allegations to the initiation agreement, VODAFONE denied that the treatment

carried out violates article 6.1 of the GDPR. It considered that this treatment was lawful

and invoked as a legal basis its section c): "the treatment is necessary for the

compliance with a legal obligation applicable to the data controller".

He explained that the legal obligation was imposed by the Sole Additional Provision of the

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

electronic communications and public communications networks (hereinafter the

Law 25/2007) that establishes:

"Telephony services through prepaid cards.



1. Mobile telephone service operators that market services

with activation system through the modality of prepaid cards,

must keep a book-registry in which the identity of the clients that

acquire a smart card with said payment method.

Operators will inform customers, prior to the sale, of the

existence and content of the record, its availability under the terms

expressed in the following number and the rights included in the article

38.6 of Law 32/2003.

The identification will be made by means of a document accrediting the

personality, recording in the registry book the name, surnames and

nationality of the buyer, as well as the number corresponding to the document

identification used and the nature or name of said document. In it

course of legal persons, [...].

2. From the activation of the prepaid card and until the obligation to

conservation referred to in article 5 of this Law, the operators will cede

the identification data provided for in the previous section, when for the

fulfillment of their purposes are required by the authorized agents, the

members of the State Security Forces and Bodies and the Bodies

Police of the Autonomous Communities with competence for the protection

of persons and property and for the maintenance of public safety, the

National Intelligence Center personnel in the course of investigations

of security on persons or entities, as well as officials of the

Deputy Directorate of Customs Surveillance.

3. The identifying data will be subject to the provisions of this Law,

regarding the systems that guarantee their conservation, not manipulation or

illegal access, destruction, cancellation and identification of the authorized person.

[...]". (The underlining is ours)

Section 3 of the Additional provision refers to other precepts of Law 25/2007

as articles 8 and 9. Article 8, "Data protection and security" provides:

"1. The obligated subjects must identify the personnel especially

authorized to access the data object of this Law, adopt the measures

technical and organizational that prevent its manipulation or use for different purposes

of those included in it, its accidental or illegal destruction and its loss

accidental, as well as its storage, treatment, disclosure or access not

authorized, subject to the provisions of Organic Law 15/1999, of 13 December

December, and in its implementing regulations.

2. Obligations relating to measures to guarantee the quality of the

data and the confidentiality and security in the treatment of the same will be the

established in the Organic Law 15/1999, of December 13, and its regulation of

development.

3. The level of protection of the stored data will be determined according to

in accordance with the provisions of Organic Law 15/1999, of December 13, and

in its development regulations.

4. The Spanish Data Protection Agency is the public authority

responsible for ensuring compliance with the provisions of the Organic Law

15/1999, of December 13, and the development regulations applicable to

data contemplated in this Law." (The underlining is ours)



Article 9 of Law 25/2007, "Exceptions to the rights of access and cancellation"

provides in its section 2:

"The data controller will deny the exercise of the right to

cancellation under the terms and conditions set forth in Organic Law 15/1999,

of December 13.” (The underlining is ours)

References to Organic Law 15/1999 on the Protection of Personal Data

Personal (LOPD) must now be understood as made to the RGPD and the LOPDGDD.

The processing of personal data that operators carry out under the Law

25/2007 is subject, in any case, to the regulations for the protection of personal data.

staff. This is confirmed by the Council of State in its Opinion 32/2007, of

02/22/2007, issued in relation to the Data Preservation Bill

relating to electronic communications and public communications networks

in which, with regard to the data processed in application of the Provision

Unique Additional, mentions, reiterating it, the criteria of the Legal Office of the AEPD

in his report:

"The keeping of the aforementioned book-registry will suppose a treatment of data, as

points out the AEPD, which at all points must be in accordance with the provisions of

Organic Law 15/1999; However, specialties may be established or

exceptions in those aspects in which that organic law allows the

they are established by law (for example, article 6.1 and 11.2.a).”

2. In view of what was alleged by the defendant in defense of the legality of her conduct -

allegations that are set forth in detail in point 2, section (i) A of the Antecedent

Sixth of this resolution - it corresponds to examine what is the content and the reason for being

of the obligation that the Sole Additional Provision of Law 25/2007 imposes on

telephone operators, in this case VODAFONE.

The need to determine the scope of this legal obligation derives from the fact that it is in

it, in connection with article 6.1.c) of the GDPR, on which it is intended to base the

legality of the treatment object of the claim and that the defendant has referred to

the Sole Additional Provision as “the yardstick to be taken by

Vodafone and the rest of the operators.”

The purpose pursued with the obligation contained in the aforementioned provision is

contribute to the fight against crime, providing the authorities that have the

power to ensure public safety of an instrument that allows them to

control the use of these devices for criminal purposes. The Preamble of the Law

25/2007, section II, penultimate paragraph, says:

"The provisions contained in the final part include content

various. On the one hand, and in order to be able to establish instruments to

control the use for criminal purposes of mobile telephone equipment

acquired through the prepaid modality, it is established, as an obligation of

the operators that market said service, the keeping of a register with the

identity of the buyers. (The underlining is ours)



Regarding the content of the imposed obligation, it is noted that it is not reduced to the fact that the

operators leave a record in a record book of the "identity" of the person who

acquires a prepaid card (“keep a record book in which the identity of the

customers who purchase a card"). The standard does not only oblige the operator to

keep a record book with the "identity" of the smart card purchaser. That

conduct is preceded by a double obligation to which the operator is subject

responsible for the treatment: the "identification" of the acquirer of the prepaid card and the

use to effect such “identification” of a specific medium (“through a

document accrediting personality").

The dictionary of the Royal Academy of the Spanish Language (RAE) defines the term

“identification” as “action and effect of identifying or identifying oneself” and the term

“identify” as “Recognize if a person or thing is the same as what is supposed or

seeks." The term "identity" (in its second meaning) as a "set of traits

characteristic of an individual or a community that characterize them in front of the others”.

Thus, it is concluded that the Additional provision examined obliges the operator, with

prior to the collection of personal data in the record book, to "recognize" that

the identity data that the acquirer of the smart card has provided you

coincide, are the same, that appear in the document accrediting your

personality. In short, in the context in which the provision is applicable

Unique additional -that of the acquisition of prepaid cards- the obligation to

"identify" that falls on the operator translates into "recognize" if the data of

identity, that is, the elements or traits with which the identity has been characterized before him.

person who intends to acquire a smart card - the name, surname, number of the

identification document provided and nature of the document and even its image

physical - are those that appear in the "document" "accrediting personality".

Law 25/2007 obliges the operator to identify, to “Recognize if a

person [...] is the same as supposed [..].”, is carried out through a

"document accrediting personality". In our legal system that

This document is, par excellence, the "national identity document" or "DNI", the only one that

by itself proves indubitably the identity of its owner.

Organic Law 4/2015, of March 30, on the protection of citizen security (in

onwards Organic Law 4/2015) establishes in its article 8, framed in Chapter II,

"Documentation and personal identification":

“Accreditation of the identity of Spanish citizens.

1. Spaniards have the right to be issued the National Document of

Identity.

The National Identity Document is a public and official document and will have
the protection granted to them by law. It is the only document with
sufficient value by itself for the accreditation, for all purposes, of the
identity and personal data of its owner.
2. The National Identity Document will include the photograph and the signature of your
owner, as well as the personal data determined by regulation,
that they will respect the right to privacy of the person without, in any case,
may be related to race, ethnicity, religion, beliefs, opinion, ideology,
disability, sexual orientation or identity, or political or union affiliation. The

support card of the National Identity Document will incorporate the measures of
security necessary for the achievement of quality conditions and
inalterability and maximum guarantees to prevent its falsification. (The underline
is ours)
Organic Law 4/2015 also mentions, as means of identification
personal, these documents: The "Passport of Spanish citizens", regulated in the
article 11 that provides “1. The Spanish passport is a public, personal document,
individual and non-transferable that, unless proven otherwise, proves the identity and
nationality of Spanish citizens outside of Spain, and within the territory
national, the same circumstances as non-resident Spaniards.” And that
certify the identity of foreign citizens under the terms of article 13.
In turn, Royal Decree 1553/2005, of December 23, which regulates the

issuance of the national identity document and its electronic signature certificates,

whose last update is 05/30/2015 (hereinafter, the Royal Decree

1553/2005) says in its article 1:

"1. The National Identity Document is a personal and

non-transferable issued by the Ministry of the Interior that enjoys the protection that

public and official documents are granted by law. Its holder will be obliged

to the custody and conservation of the same.

2. Said Document has sufficient value, by itself, to prove the identity

and the personal data of its owner that are recorded therein, as well as the

Spanish nationality of the same.

3. Each National Identity Document will be assigned a personal number

which will be considered a personal numerical identifier of character

general.

4.[...]" (The underlining is ours)

For its part, article 11 of the Royal Decree, under the heading "Content" indicates:

"The National Identity Document will graphically collect the following data

of its holder: On the obverse: [...] Personal Number of the National Document of

Identity and verification character corresponding to the Identification Number

Fiscal." (The underlining is ours)

The explicit reference that the Additional provision of Law 25/2007 makes to the means of

identification, to the "document" accrediting personality, presupposes that the

operator has to physically access the document. The use of

the photocopy, since it lacks the security guarantees enjoyed by the

original document. Regarding the DNI, we refer to the last paragraph of the

article 8.2 of the Organic Law 4/2015, reproduced above, and article 10 of the

Royal Decree 1553/2005 "Characteristics of the support card" which says:

"1. The material, format and design of the support card of the National Document of

Identity will be determined by the Ministry of the Interior, taking into account in its

elaboration the use of procedures and products conducive to the

achievement of quality and inalterability conditions and maximum guarantees

to prevent its forgery. An electronic chip will be incorporated into the object of



enable the computer utility referred to in article 1.4 of this Royal

Decree."

In line with the foregoing, it should be noted that the allegation of

VODAFONE, according to which the third party that intervened in the contracting did not contract

the line "in the name of the claimant" but in his own name. The defendant insists on

that idea on several occasions and takes into consideration for this that the third party that

intervened in the contracting was identified with the NIF of the claimant, but not with the

name and surname of the claimant but with that of B.B.B.. However, it

determining factor is that the NIF used by the purchaser of the prepaid product was that of the

claimant and that data has "per se" value to fully identify its owner with

all the data contained in it, also the name and surname. While the

names and surnames can coincide in several subjects, the NIF is exclusive of the

person to whom it is assigned.

3. In consideration of the foregoing, it is obligatory to conclude that article 6.1.c) of the

GDPR, in connection with the Unique Additional Provision of Law 25/2007, is a

valid grounds for the legality of the treatment that telephone operators make

of the personal data of which card purchasers are holders

intelligent, as long as the data processing carried out by the operator is

adheres to and has the sole purpose of complying with the provisions of that law.

In this sense, it should be noted that section c) of article 6.1 of the GDPR, in connection

with Law 25/2007, does not cover the treatment that the operators carry out, for other

purposes other than that pursued by the Unique Additional provision, of the data

collected in compliance with that provision, such as those related to

the development and execution of the contract. The treatments eventually carried out by a

operator for purposes other than those contemplated in the Additional provision

aforementioned, must be covered by one of the other legal bases

described in article 6.1. of the GDPR, but not in section c) in connection with the

Law 25/2007.

Likewise, it must be concluded with respect to the assumption that is being examined here that it is not

possible to protect the legality of the treatment that VODAFONE made of the NIF of the

claimant on the legal basis of section c) of article 6.1 of the GDPR in relation to

with the obligation imposed in the Sole Additional Provision of Law 25/2007.

The obligation imposed in the aforementioned provision of Law 25/2007, connected with the

Article 6.1.c) of the GDPR, authorizes the operators, exclusively, to process the data

of which the persons who acquire a prepaid card are holders; by way of

that the processing of data that does not identify the purchaser of this type of service

is outside the coverage of the aforementioned Additional provision.

As we have previously indicated, in the data processing that the operators

carried out in compliance with Law 25/2007, it is mandatory to always respect the

data protection regulations. Moreover, Law 25/2007 expressly provides that

apply to the data mentioned in it the obligations established by the

GDPR (formerly LOPD) to guarantee the quality of the data. In the context of the

Unique Additional provision of Law 25/2007, the inaccuracy of the data that the

operator links the purchaser of a prepaid card -especially if the data is a



DNI, since it unequivocally identifies a person- prevents this treatment from being

considered lawful on the basis of article 6.1.c) of the GDPR in connection with the provision

of Law 25/2007. Provision that, as has been said, imposes on the operator the

obligation to collect data that identifies the purchaser of the smart card

but not the data of third parties.

The reasons stated lead to rejecting VODAFONE's claims to the

agreement to initiate this procedure in which it maintains that the circumstance of

that the NIF data is erroneous is irrelevant and in no way affects the legality of the

treatment carried out. The defendant said:

"Vodafone is obliged by Law 25/2007 to treat the "corresponding number

to the identification document used" by the buyer of the prepaid card;

A different matter is that said number turns out to be wrong or has been used

through fraud by a third party, but this may not imply, in any case,

a violation of article 6.1 of the GDPR.” (The underlining is ours)

On the other hand, VODAFONE has recognized in its allegations to the start-up agreement

(third allegation) that the NIF data of the claimant who was subject to treatment

linked to the prepaid line did not belong to the purchaser of the card. The entity has

saying:

“[...] there may be cases, such as this one, in which Vodafone processes data

personal that does not belong to the prepaid card applicant, but to a third party

(the Claimant). This is what has happened in this case: it is evidence and not the

we deny." (The underlining is ours)

In short, the conduct of VODAFONE that is the object of analysis constitutes a

illegal treatment of the claimant's NIF and violates article 6.1 of the GDPR. The

claimed tried the NIF of the claimant and not that of the purchaser of the prepaid service,

only data that it was empowered to collect in accordance with the legal obligation whose

compliance has invoked: the Sole Additional Provision of Law 25/2007.

4. Once the existence of unlawful conduct by VODAFONE has been proven - the treatment

of the NIF of the claimant without a legal basis- the question focuses on determining whether in such a

conduct may give rise to penalizing administrative responsibility.

4.1. As mentioned by the defendant in her statement of allegations, the responsibility

objective is proscribed in our legal system. In Administrative Law

sanction governs the principle of guilt, so the subjective element or

culpability is an indispensable condition for liability to arise

sanctioning. The Constitutional Court, among others, in its STC 76/1999, has

declared that administrative sanctions participate in the same nature as

criminal, as it is one of the manifestations of the ius puniendi of the State, and that, as

requirement derived from the principles of legal certainty and criminal legality

enshrined in articles 9.3 and 25.1 of the CE, its existence is essential to

impose them

Regarding the guilt of the legal person, it is appropriate to cite STC 246/1991, 19

of December 1991 (F.J. 2), according to which, with respect to legal persons, the

subjective element of guilt must necessarily be applied differently to

as it is done with respect to natural persons and adds that "This different construction

of the attribution of the authorship of the infringement to the legal entity arises from the very

nature of legal fiction to which these subjects respond. Missing in them the

volitional element in the strict sense, but not the ability to break the rules to which

which they are subjected Infringement capacity and, therefore, direct reproach that

derives from the legal right protected by the rule that is infringed and the need for

such protection is really effective [...]" (The emphasis is ours)

Law 40/2015 on the Legal Regime of the Public Sector establishes in article 28,

"Responsibility":

"1. They may only be penalized for acts constituting an infringement

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

recognize the capacity to act, the groups affected, the unions and entities

without legal personality and independent or autonomous estates, which

are responsible for them by way of fraud or negligence."

In the light of this precept, the sanctioning responsibility can be demanded by way of

fraud or negligence, being sufficient in the latter case the mere non-observance of the duty of

careful.

4.2. VODAFONE dedicates the third allegation of its allegations to the start-up agreement to

defend that, with respect to the unlawful conduct that has been accredited,

No guilt of any kind was involved on his part. Accordingly, request the file

of the file due to the absence of the necessary element of guilt.

The defendant has tried to justify the absence of guilt in her conduct - the

registration of the prepaid line linked to the NIF of the claimant - with various arguments,

as the criminal action of a third party (the contracting party), who would have circumvented the VODAFONE controls. Also in the existence of an error not attributable to the entity. He has stated that “[...] there may be cases, such as this one, in which Vodafone processes personal data that does not belong to the applicant for the prepaid card, but to a third party (the Claimant). [...] we would be faced with cases in which the applicant (the Third Party), using tricks and using his experience to his advantage criminal, has managed to evade the controls established by Vodafone, causing the human error at the Point of Sale.”

The decision to file a disciplinary file may be based on the absence of the element of guilt when the person responsible for the unlawful conduct had acted with all the diligence that the circumstances of the case require. This is recognized by the demanded when echoing the pronouncement of the STS of January 23, 1998 in which, as stated, the Court declares that "for the exculpation the invocation of the absence of guilt will suffice, but it will be necessary that used the diligence that was required by the person claiming its non-existence.”

In compliance with the principle of guilt, the AEPD has agreed on numerous occasions the file of sanctioning procedures in which the element of the guilt of the offending subject. Cases in which, despite the existence of a unlawful behavior, it had been proven that the person responsible had acted with all the diligence that was required, for which reason no fault was appreciated



some in his conduct. This has been the criterion maintained by the Contentious Chamber

Administrative, section 1, of the National Court. They can be cited, because they are very

illuminating, the following sentences:

- SAN of April 26, 2002 (Rec. 895/2009) which says:

"In effect, it is not possible to affirm the existence of guilt from the result and this is

what the Agency does when maintaining that by not having impeded the security measures

the result is guilt. Far from it what must be done and is missed in the

Resolution is to analyze the adequacy of the measures from the parameters of

average diligence required in the data traffic market. Well, if you work with full

diligence, scrupulously fulfilling the duties derived from an act

diligent, it is not possible to affirm or presume the existence of any fault." (The underlining is

of the AEPD)

- SAN of April 29, 2010, Sixth Legal Basis, which, regarding a

fraudulent contracting, indicates that "The question is not to determine whether the appellant tried to

the personal data of the complainant without their consent, as if

whether or not you used reasonable diligence in trying to identify the person with

who signed the contract. (The underlining is from the AEPD)

4.3. At this point, it is worth remembering again what STC 246/1991 has

Said with regard to the guilt of the legal entity: that it does not lack the

"ability to break the rules to which they are subjected". "Capacity of

infringement that derives from the legal right protected by the norm that is infringed and the

need for said protection to be really effective [...]". (The underlining is

our)

In connection with the foregoing, reference must be made to article 5.2. of the GDPR (principle of

proactive responsibility), according to which the person responsible for the treatment will be

responsible for compliance with the provisions of section 1 - so here

interested, of the principle of legality in relation to article 6.1 of the GDPR- and capable of

demonstrate its compliance. The principle of proactivity transfers to the person in charge of the treatment the obligation not only to comply with the regulations, but also to be able to demonstrate such compliance

Article 5.2 is developed in article 24 of the GDPR, which obliges the controller to adopt the appropriate technical and organizational measures "to guarantee and be able to demonstrate" that the treatment is in accordance with the GDPR. The precept establishes:

"Responsibility of the data controller"

"1. Taking into account the nature, scope, context and purposes of the treatment, as well as risks of varying probability and severity for rights and freedoms of natural persons, the data controller apply appropriate technical and organizational measures in order to guarantee and be able to Demonstrate that the treatment is in accordance with this Regulation. said measures will be reviewed and updated when necessary.

2. When they are provided in relation to the treatment activities, the measures referred to in paragraph 1 shall include the application, for part of the person responsible for the treatment, of the appropriate protection policies of data.



3. Adherence to codes of conduct approved under article 40 or to a certification mechanism approved under article 42 may be used as elements to demonstrate compliance with obligations by the controller." (The underlining is ours)

Article 25 of the GDPR, "Data protection by design and by default",

establishes:

“1.Taking into account the state of the art, the cost of the application and the

nature, scope, context and purposes of the treatment, as well as the risks of

varying probability and severity involved in the treatment for the rights and

freedoms of natural persons, the data controller will apply, both

at the time of determining the means of treatment as at the time

of the processing itself, appropriate technical and organizational measures, such as the

pseudonymization, designed to effectively apply the principles of

data protection, such as data minimization, and integrate safeguards

necessary in the treatment, in order to meet the requirements of this

Regulation and protect the rights of the interested parties.

2.[...]” (The underlining is ours)

It is worth asking what are the due diligence parameters that VODAFONE

should have observed in relation to the behavior examined. The answer is that the

diligence that he should have observed is that which was necessary to fulfill the obligations

imposed by the Unique Additional Provision of Law 25/2007 in relation to the

Articles 5.2, 24 and 25 of the GDPR, in light of the doctrine of the National Court and the

jurisprudence of the Supreme Court.

It is fully applicable to the case, despite having been issued during the validity of the Law

Organic Law 15/1999, the SAN of 10/17/2007 (Rec. 63/2006), which, after referring to

that the entities in which the development of their activity entails a continuous

processing of customer data and third parties must observe an adequate level of

diligence, says: "[...] the Supreme Court has been understanding that there is imprudence

whenever a legal duty of care is neglected, that is, when the offender does not

behaves with the required diligence. And in assessing the degree of diligence must

especially the professionalism or not of the subject should be considered, and there is no doubt that,

in the case now examined, when the appellant's activity is constant and

copious handling of personal data must insist on rigor and

Exquisite care to comply with the legal provisions in this regard". (The underline

is from the AEPD)

VODAFONE maintains that, in compliance with the obligation imposed by the Law

25/2007, observed all the diligence that was required. To verify this statement

nothing better than examining the documentation that is in the file and accredits

what were the measures effectively adopted by that operator.

VODAFONE was asked in the test phase how it could prove to the AEPD that

the point of sale collected from the person who requested the contracting of the prepaid line

your original identity document (not a photocopy); that the point of sale verified your

identity and that it collected the client's identity data from the aforementioned document. The

The defendant replied that the distributor SERCOM had been bound in the contract of



Wholesale Distribution subscribed with VODAFONE to transfer to the point of sale the

essential obligation to identify the client/buyer by means of their card

original identification and that, in turn, this obligation had been transferred to the contract

signed between the SERCOM distributor and the retail point of sale,

***ESTABLISHMENT.1.

It can thus be verified that the measures that the claimed operator had articulated

consisted solely of having established contractual clauses by virtue of the

which subjects are involved in the processing of the data of a purchaser of

a prepaid card -several subjects, since the person in charge of treatment, the Distributor

Wholesaler, followed by several sub managers, the points of sale, in this case

concrete *** ESTABLISHMENT.1 - are obliged to act in accordance with the Law.

We are dealing with mere contractual stipulations. The truth is that VODAFONE has not

not even been able to provide the documents that, in compliance with the provisions of the

Wholesale Distribution contract, should have in his possession, as is the case of the

certificate to be issued by the wholesale distributor.

Thus, in the sixth Proven Fact it is stated that the Wholesale Distribution contract

signed between VODAFONE and SERCOM, established (clause 12.2) that SERCOM "will give

transfer of all obligations regarding the protection of personal data

personnel to Retail outlets and will certify having transferred these

obligations by signing a standard certificate attached as

document IV.”.

Requested in evidence from VODAFONE the certificate issued by SERCOM under the

the aforementioned stipulation, the defendant responded by providing a form, annex IV to the

contract, in which there is no mention of SERCOM: in the document provided

The details of who should be the certifier (SERCOM) are not filled in.

The spaces for your NIF, name, address and information of your

representative; there is no SERCOM stamp or signature but a VODAFONE stamp

stamped twice and a signature with no indication of who it belongs to.

Annex II to the contract between SERCOM and VODAFONE, which bears the heading "Collection

of data. Wholesale distribution contract”, says that it contains the instructions

regarding compliance with the Sole Additional Provision of Law 25/2007, regarding

of (i) the face-to-face identification and data collection of customers who purchase a

Prepaid Card or a Prepaid Pack prior to the sale and (ii) the information

to them in the terms described in the aforementioned Law, all in accordance with

the provisions of clause 11.2 of the Wholesale Distribution Agreement of which the

Annex brings cause.

It is verified that Annex II to the Wholesale Distribution contract says in its

“In-person Identification and Data Collection of the

first stipulation,

Customer/Buyer":

"1. The WHOLESALER must transfer to the retail Point of Sale through the

subscription of an agreement that includes obligations related in the present

annex, the essential obligation to identify PRESENTIALLY the

Customer /Buyer

original identification card. * The

Documentation to be presented by natural persons according to their nationality and

through his



situation is as follows: -For Spaniards: DNI or NIF. -For citizens of the

European Community ID, Residence Card and Passport are accepted. -For

Citizens from outside the European Community: Passport or NIE. [...].” (He

underlined is ours)

However, in the contract for the retail distribution of telephony products signed

between SERCOM and ***ESTABLECIMIENTO.1, (document number 6 of those provided

in test phase) for the sale of VODAFONE prepaid services is not

does not include any reference to the identification document that is collected from the

buyer must be the original (we refer to article 4.1.c) of the contract, see

Proven Fact seventh, third paragraph).

Regarding the controls planned by VODAFONE to verify compliance that

managers and sub managers make the obligations imposed on them by

contracts, it was requested in the test phase to detail which ones it had

established in order to verify that the contracts with the retail outlets were

adjusted to law.

VODAFONE explains that the controls consisted, on the one hand, of the certificate that

SERCOM issued according to the model in Annex IV to the Wholesale Distribution contract,

in compliance with the obligation established in its clause 12.2. About this

certificate, as has been exposed, despite the fact that it was requested in the test phase, the

The defendant has not provided it, since the document that it sends does not include any

reference to SERCOM so it is difficult to certify something through it. By

another, VODAFONE referred to the fact that the distributor, in accordance with clause 11.1 of the

Wholesale Distribution contract, was obliged to inform VODAFONE of the

identity of the points of sale with which it entered into contracts and on which

products supplied to you. In relation to this measure, it is unknown what

In this way, with that single measure, VODAFONE could know, and even less control, if the

points of sale followed or did not follow the identification protocol of the purchasers of the

prepaid cards provided for in the contract with the Wholesale Distributor.

The lack of diligence shown by VODAFONE in its

obligation to keep a record of processing activities (RAT). this lack

has a direct impact on the probability that the defendant adopts the measures

appropriate to guarantee compliance with the principle of legality with respect to data

such as the NIF, whose treatment is not reflected in the RAT that the entity

He has provided.

Article 30 of the GDPR requires that the RAT describe, among others, "the

categories of personal data". In response to the request made to the defendant in

test phase to provide that record, the document you have provided refers to

exclusively on the activity of the Distributors-Franchisees and does not make any

reference to the NIF data or to the identification documents that must be collected with

occasion of the sale of prepaid products. Nor does it mention as the legal basis of the

treatment which has been invoked in its allegations as a legal basis for the

treatment (article 6.1.c, of the GDPR in relation to the Additional provision of the

Law 25/2007). On the contrary, in the RAT provided it is contemplated as a legal basis that

"People have given their consent for the processing of their personal data

for one or more purposes.



Thus, the privacy policy of VODAFONE that it says was mocked by the

criminal action by a third party, is reduced, in practice, to including in the

contracts signed with the wholesale distributor and between it and the points of sale

obligation to identify the purchaser of the prepaid service in accordance with the provision

Additional Law 25/2007. That, with the qualification that the contract with

***ESTABLISHMENT.1 did not require that the identification document be the original.

The additional obligations that are incorporated into the Wholesale Distribution contract,

such as the certificates that the distributor had to issue, have not been fulfilled.

The adoption of any specific measure is not contemplated in accordance with articles

5.2, 24 and 25 of the GDPR to prove compliance with the obligation that arises

for VODAFONE of Law 25/2007. In short, there has been no conduct

proactive materialized in the adoption of appropriate technical and organizational measures

to effectively apply the data protection principles.

It therefore follows that, as indicated in the initiation agreement, the security policy

of VODAFONE is clearly ineffective and insufficient, it is well below the

possibilities that current technical development offers and does not take into account the

evident risk that contracting the services it sells represents for

the rights and freedoms of people

4.4. Finally, the allegations made by VODAFONE on purpose are reproduced

of the considerations that were included in the agreement to initiate this

procedure regarding the infringement of article 6.1 of the GDPR at hand.

It was said in the initiation agreement that, by virtue of the principle of proactive responsibility

(article 5.2 GDPR), the data controller must be in a position to

demonstrate that the data processing carried out complied with the principles

of data protection, in particular the principle of legality. which meant that

should be able to prove that he had identified the person with whom he hired

through the means required by Law 25/2007 and that this person was the holder of the NIF

treatment object.

It was added that the defendant, in her response to the request for information from the

Inspection Sub-Directorate, prior to admitting the claim for processing, had

provided this Agency with various documentation with which he intended to justify that his

action was adjusted to law but, however, did not provide any proof

that demonstrates that, when contracting the line associated with the NIF of the

claimant, acted with the diligence that was required in compliance with the principle of

legality. She had limited herself to stating that the third party that contracted with her and

identified with the NIF of the claimant "satisfactorily passed the

security" of the company "because to carry out the registration of a prepaid line

requires the display of an official identification document before the agents of the

physical stores. (The underlining is ours)

It was then said that the security policy followed by the defendant did not allow her to

prove, not even indicatively, that the store agents collected the

contracting third party the display of an identification document; that he exhibited it;

that the defendant, through its agents, checked it against the identity data



provided and that the result of that comparison confirmed that the contracting party was the

owner of the data provided as his, so that policy was not consistent

with the proactive attitude that the person in charge must adopt to fulfill the obligation

imposed by the GDPR to respect the principle of legality.

Reference was also made to the considerations on the principle of proactivity

offers Opinion 3/2010, of the Article 29 Working Group (GT29) -WP 173-

issued during the validity of the repealed Directive 95/46/EEC, but whose

reflections are applicable today, in which it is stated that the "essence" of the

Proactive responsibility is the obligation of the data controller to apply

measures which, under normal circumstances, ensure that, in the context of

processing operations, data protection regulations are complied with

and in having available documents that demonstrate to the interested parties and the

Control authorities what measures have been adopted to achieve compliance

of data protection regulations.

For all these reasons, in the opening agreement it was considered that the security policy of

VODAFONE was clearly ineffective and insufficient and it was also noted that this

The lack of solidity of the measures affected the graduation of the sanction of a fine

The circumstance of article 83.2.d) of the GDPR must be applied as an aggravating circumstance

regarding the "degree of responsibility of the controller (...) taking into account the

technical or organizational measures that they have applied under articles 25 and

32."

Faced with these considerations made by the AEPD in the initiation agreement, which

reiterate, VODAFONE has stated the following:

"[...]if the Agency intends to increase the requirements in terms of identification

incorporating obligations of conservation and technical verification of

documents, what proceeds is to approve rules to that end [...] and later, in

where appropriate, penalize the operator that does not apply them, but what is not

according to law is to try to directly use the disciplinary route as

method of setting the required security parameters."

"In fact, in this specific case there is no possibility for the

private operators to check if the ID number corresponds

effectively to the person who claims to be the owner and accredits it with a document

that can be manipulated. Otherwise, it would go against the regulations of

data protection, and that is that the only way to avoid fraud like the one that has

origin of this file would be that Vodafone had access to a database

data that would allow verifying that if the ID number used by the

applicant actually belongs to the applicant in question." (The underlining is

our)

The reflections that were made in the opening agreement, which are reiterated in this

resolution, are not, as VODAFONE argues, an attempt by the Agency to "increase"

“the requirements in terms of identification incorporating obligations of

preservation and technical verification of documents”. Contrary to what the claimed

maintains that the AEDP has limited itself to examining the sufficiency of the measures that

VODAFONE had established to prove the identity of the person who contracts with it



a prepaid service in compliance with the Additional provision of Law 25/2007, to

in light of articles 5.2, 24 and 25 of the GDPR.

Therefore, in view of the foregoing, it must be concluded that VODAFONE is responsible

of a violation of article 6.1. of the GDPR typified in article 83.5.a) GDPR,

precept that says:

Violations of the following provisions will be penalized, according to

with paragraph 2, with administrative fines of maximum EUR 20,000,000

or, in the case of a company, of an amount equivalent to a maximum of 4%

of the overall annual total turnover 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;”.

Article 72.1.b) of the LOPDGDD qualifies as a very serious offense "The treatment 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.” The limitation period

for very serious offenses (article 72.1) is three years.

SAW

Violation of article 6.1 of the GDPR: Consultation of the ASNEF file linked to the NIF of the

claimant:

In the agreement to initiate this disciplinary procedure, VODAFONE was identified as

ESPAÑA, S.A.U., with NIF A8090739, as responsible for an alleged infringement

of article 6.1. of the GDPR specified in having consulted the solvency file

ASNEF using the NIF of the claimant without a circumstance concurring

legitimizing that treatment. Subsequently, the motion for a resolution confirmed

VODAFONE ESPAÑA, S.A.U.

However, in the EQUIFAX document, dated 12/11/2020, that the claimant

attached to your claim, accrediting the consultation to the ASNEF file on 09/15/2020

linked to his NIF, it is clear that the person who made this query was the company VODAFONE

ONO, S.A.U. This company, whose NIF is A62186566, is a different legal entity

of the one identified as the claimed party of this proceeding.

Article 28 of Law 40/2015, of October 1, on the Legal Regime of the Sector

Public (LRJSP), under the heading "Responsibility" provides in section 1:

"Only those that may be penalized for acts constituting an administrative infraction

physical and legal persons, [...], who are responsible for them by way of

fraud or fault."

Therefore, with regard to the infringement of article 6.1 of the GDPR specified in

having treated the claimant's NIF without legitimacy to consult a file of

solvency on 09/15/2020, the filing of this file must be agreed

penalized for not being attributable such conduct to the claimed party, VODAFONE

ESPAÑA, S.A.U., with NIF A80907397.

It is also indicated that, as long as it has not prescribed, nothing prevents the opening of a disciplinary proceedings against VODAFONE ONO, S.A.U., as responsible for a violation of article 6.1. of the GDPR derived from the treatment of the NIF of the claimant without legal basis specified in the consultation of a solvency file.

As indicated in the agreement to initiate this procedure, article 72 of the LOPDGDD qualifies the infringement of article 6.1 of the GDPR as very serious and establishes for it a limitation period of three years, so that the aforementioned infringement It will prescribe on 09/15/2023.

VII

Infringement of article 17 of the GDPR

1. In the agreement to start the disciplinary procedure, VODAFONE was attributed an infringement of article 17 of the GDPR for not having attended, in the terms established in Regulation (EU) 2016/679, the right of deletion exercised by the claimant with respect to the data of his NIF, despite the fact that the claimed operator came obligated to suppression in accordance with section 1.d) of that provision. Infraction that the claimed has rejected.

We will refer, first of all, to the facts related to this conduct. contrary to the GDPR:

The claimant requested VODAFONE to delete the data from her NIF on 01/24/2021. The claimed did not attend to her right until 05/27/2021, when the more than four months from the request and after it was known by the AEPD, in the framework of the transfer actions of the Sub-directorate of Inspection, which existed a claim against it presented by affected before this Agency.

The claimant provided VODAFONE with annexes to her request to delete the date 01/24/2020 sent to the email address derechosprotecciondatos@vodafone.es, these documents: the signed application, a copy of your ID and the extension of the complaint filed with the Police. The copy of the police report had been sent to VODAFONE days before, with an email dated 12/21/2020.

VODAFONE responded by email dated 01/26/2021 in which said:

"[...] In view of your request, in which you exercise the right [...] We regret inform you that this entity cannot generate the deletion of the data requested since they are necessary to provide the service to the line prepaid ***PHONE.1, we understand the purpose of your request, without However, and in case of not recognizing the product, we could generate a rectification of data so that the service is recorded in your name and you can carry out use thereof; We emphasize that prepaid products cannot be deactivated, failing that we can wait for the card to expire (Approximately estimated expiration date to June 2021 if not



generate recharges), after that you could again request your right to suppression." (The underlining is ours)

The defendant, in addition to stating in her response that she "cannot" proceed to the deletion of the data because it was necessary to provide the service to the prepaid line and "emphasize" that prepaid products cannot be deactivated, informed the

claimant that they should wait for the prepaid card to expire, which is

It would foreseeably occur, provided no recharges were generated, in June 2021.

He informed him that, on that date, he should once again exercise his right to

suppression. VODAFONE also offered this alternative that qualifies itself:

put the line to your name. In other words, rectify the name and surname data

provided by the third party that contracted with her and that were recorded in their systems and

replace them with those of the claimant.

VODAFONE responded on 02/03/2021 to an email from the complainant dated

02/1/2021 in which he asked if, as he had been informed through Facebook, the

operator had already proceeded to suppress his NIF. In this email dated 02/03/2021

VODAFONE reiterated its refusal to comply with the right of deletion and said:

"(...) In response to your email, we must inform you that the hotline

***TELEPHONE.1 corresponding to the file registered with your phone number

National Identity Document was expired by our fraud area with the

purpose of avoiding any type of use, however, it still registers in

our system and will only be disconnected until June 2021, which

makes it impossible for your data to be deleted from our system. (...)

Finally, we make the clarification that your request (Deletion of data)

It can only be attended to until the previously stated date (June

2021), therefore it is necessary that you send us this request at the end of the month

exposed. (...)" (The underlining is ours)

From the message it can be clearly inferred that VODAFONE recognized that the NIF linked to

the prepaid line did not belong to the contracting party but to the claimant, since the line "was

expired" by the "fraud" area of the operator; but, despite this, the personal data

of the claimant will not be deleted until June, when the prepaid line is

disconnected.

2. The defendant has denied that it has violated article 17 of the GDPR and has stated that, despite the fact that the "wording" of their answers was "unfortunate", respected the applicable regulations.

You have argued that, pursuant to Article 17 of the GDPR, you were not required to to suppress the NIF data of the claimant because the treatment of this data was not illicit. And he has justified his statement, in line with what is alleged in this proceeding, in that the treatment of the DNI provided by the applicant for the prepaid card "[...] comes imposed by the Sole Additional Provision of Law 25/2007". Furthermore, he adds that "Vodafone does not keep this data (DNI number) related to the identity of the Claimant, but with the identity (name and surname) of the Third Party". We refer to what has already been stated in the First Allegation to avoid unnecessary repetitions



It has also argued that two of the exceptions in section 3 of the Article 17 of the GDPR:

The one provided for in letter b), on which it says that "The treatment of the DNI number provided by the Third Party was necessary for Vodafone to comply with a legal obligation", which is the one imposed by the Sole Additional Provision and article 5, both of Law 25/2007. It considers that, according to the Additional provision "the Telephone operators are obliged to collect certain data from the applicant of a prepaid card, including "the number corresponding to the document identifier used "", and that, in accordance with the rules on data conservation of article 5 of Law 25/2007, was obliged to keep the DNI "provided by the

contracting of the prepaid card”.

The second exception to the application of section 1 of article 17 of the GDPR that judgment of the claimed party would be applicable is that of section e) of article 17, on which comments that it was "authorized to keep the data provided by the Third Party in the event that in the future said data is necessary to formulate, exercise or defend against any claim. In this sense, it becomes important again fact that Vodafone had not associated the Complainant with the identity, but rather with that of the Third Party, that is, who registered the prepaid card, which had also been flagged as "fraud".

3. Law 25/2007 establishes in article 9, “Exceptions to the rights of access and cancellation":

"1. [...].

2. The data controller will deny the exercise of the right of cancellation in the terms and conditions provided in the Organic Law 15/1999, of December 13.” (The underlining is ours).

Referral that, as has already been said, must be understood to the current regulations, the RGPD and the LOPDGDD. In turn, article 17 of the GDPR, "Right of deletion ("the right to be forgotten»)”, provides:

"1. The interested party shall have the right to obtain without undue delay from the person in charge of the treatment the deletion of personal data that concerns you, which will be obliged to delete the personal data without undue delay when one of the following circumstances occurs:

to)

[...]

d) the personal data have been unlawfully processed; [..]”

Article 17 of the GDPR is exhaustive by obliging the data controller to delete,

without undue delay, a personal data when, as it happens here, the treatment is

illegal, but, in any case, with the exception that the processing of the data is necessary

for any of the purposes detailed in section 3 of article 17 (letters a, to e).

It has been duly justified in Fundament V of this resolution that the

treatment of the claimant's NIF data carried out by VODAFONE linked to

a prepaid line violated the principle of legality because it was not covered by any

of the legal bases listed in article 6.1 of the GDPR.



On the other hand, the reasons that the defendant gave to the claimant to justify not

delete the NIF data "without undue delay", were related to alleged

technical requirements of the product contracted by the third party with the NIF of the claimant,

circumstance that is not included among the exceptions to the application of article

17.1 that contemplates article 17.3 of the GDPR.

Compliance with the obligation that article 17.1 of the GDPR imposes on the controller

of the treatment -proceed without undue delay to the deletion of the data of the

interested party when there is any of the circumstances that are related therein- not

may be subordinated or made dependent on more exceptions than those provided for in the

paragraph 3 of article 17 of the GDPR. In no case in matters related to

the operation of the business of the controller, whether of a technical nature, such as

those that the defendant claimed in the messages that she addressed to the claimant, or otherwise

nature.

It is added to what has already been stated that when VODAFONE responded, denying it, to the

The claimant's first request to delete her NIF knew that the

treatment of this data could be illegal, since two days after that

first deletion request, the existence of a

possible fraud in contracting the prepaid line.

However, before the VODAFONE email of 02/03/2021, in which it denies the

suppression of the NIF -response email to another from the claimant dated 02/01/2021 in

the one who requested confirmation of the suppression of his NIF- the claimed was fully

aware that the treatment of the claimant's NIF that was carried out was illegal

linked to the disputed line, as its fraud department had already

cataloged as such the line. Despite this, the defendant insisted on responding to the

complainant that the NIF could not be deleted because the prepaid products could not be

be deactivated and it was necessary to wait for the card to expire.

VODAFONE deletes the claimant's NIF more than four months after the

first request and does so after learning that there was a claim against

her, as a result of the actions of transfer of the Sub-directorate of Inspection of this

Agency.

The conduct of VODAFONE, which did not attend, being appropriate, the right that the

Article 17 of the GDPR recognizes the claimant, constitute a clear violation

of that norm.

In its allegations, VODAFONE denies having violated article 17 of the GDPR.

The arguments that VODAFONE invokes in defense of the non-existence of the infringement

of article 17.1. of the GDPR consist, in essence, of two exceptions to the application

of article 17.1 provided for in article 17.3 of the GDPR and in the statement that the

entity did not keep the data of the DNI object of treatment "related" to the

"identity" of the claimant, but with the "identity" of the third party who intervened in the

hiring. In particular, it states that "Vodafone does not store this data (number of

DNI) related to the identity of the Claimant, but to the identity (name and

surname) of the Third Party. We refer to what has already been stated in the First Allegation to

avoid unnecessary repetitions. “Vodafone had not associated with the identity of the



Claimant, but with that of the Third Party, that is, who registered the prepaid card, which

it had also been marked as "fraud". (The underlining is ours)

Starting with this last consideration, it should be indicated that it contains affirmations

contradictory. As stated in Fundamento V, following the RAE, the term

"identity" is the "set of characteristics of an individual or a community that

characterize them in front of the others”. In turn, according to Organic Law 4/2015, the

The identity of a Spanish citizen is accredited through the DNI, "the only document with

sufficient value by itself for the accreditation, for all purposes, of the identity and

the personal data of its owner”. And, according to Royal Decree 1553/2005 "To each

National Identity Document, you will be assigned a personal number that will have the

consideration of personal numerical identifier of a general nature.”

It therefore turns out that, by incorporating VODAFONE into its systems the data of the DNI/NIF of

the claimant was fully identified in the systems of the

claimed, and this regardless of whether or not VODAFONE associates it with a

customer number or the name and surname of the third party (B.B.B..) In turn, the

statement according to which he kept the NIF data of the claimant "related" to the

"identity (name and surname) of the Third Party". The name and surnames do not identify

fully to the third. The identity of the third party would be effectively registered in their

systems if you had your NIF (not just your name and surname), data that VODAFONE does not collected and has not registered either. Therefore, when it comes to identifying the customer the decisive thing is the DNI/NIF data.

With regard to the exceptions to the application of article 17.1 of the GDPR that, judgment of the defendant, would operate in this case, sections b) and e) of article 17.3 of the GDPR, the following is indicated

In relation to section b) of article 17.3. of the GDPR - compliance with a legal obligation that requires data processing that is imposed by the law of the Member States and applies to the controller - it is enough say that it is precisely Law 25/2007, in particular its article 9, which refers to the application of the personal data protection regulations: "The responsible for data processing will deny the exercise of the right to cancellation under the terms and conditions set forth in Organic Law 15/1999, of December 13th." (The underlining is ours)

So it is Law 25/2007, connected with article 17.3.b) of the GDPR, in which that VODAFONE seeks to exempt the application of article 17.1.d) of the GDPR, which expressly obliges the operator to observe the provisions of the GDPR when respond to requests for the deletion of the data that is processed with occasion of its application. And, in turn, in accordance with article 17.1.d) of the GDPR The deletion of those personal data whose treatment is illegal will proceed.

Nor is it acceptable as a exception to the application of article 17.1.d) of the GDPR and, therefore, as a reason to justify the refusal to delete the data of the NIF, the hypothesis of letter e) of article 17.3: that the treatment of the data was necessary “for the formulation, exercise or defense of claims.”

Consideration that seems obvious since the claims that VODAFONE could

direct in front of their managers or sub-managers of treatment, or even in front of the

third, they do not need for their justification or proof to continue carrying out a

treatment of the NIF of the claimant linked to the prepaid line, treatment that is

illicit. Even more so if one takes into account the rigor with which the CJEU interprets the term

"necessary", referring to a treatment because it rejects that "necessary" can be equated

convenient or suitable.

Based on the foregoing, this resolution concludes that VODAFONE violated article 17

of the GDPR by not proceeding to the deletion of the NIF of the claimant despite being forced to

to it in accordance with section 1.d) of that provision.

The infringement of article 17 of the GDPR that is attributed to the defendant is

typified in article 83.5.b) of the GDPR which indicates:

Violations of the following provisions will be sanctioned, in accordance with the

paragraph 2, with administrative fines of maximum EUR 20,000,000 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:

to) (...)

b) the rights of the interested parties in accordance with articles 12 to 22;"

The LOPDGDD qualifies in its article 72.1.k) as a very serious infraction "The

impediment or obstruction (...) of the exercise of the rights established in the

articles 15 to 22 of Regulation (EU) 2016/679." The limitation period for these

violations is three years.

VIII

Sanction of a fine: Determination of the amount

Article 58.2 of the GDPR attributes various powers to the control authorities

corrective measures, among which the precept mentions, section i), the imposition of a fine

administration in accordance with article 83 of the GDPR.

In this resolution it is agreed to penalize VODAFONE for the two violations of the

article 6.1 of the GDPR and the infringement of article 17 of the GDPR with separate fines

administrative.

In determining its amount, the provisions of the articles must be taken into account.

83.1 and 83.2 of the GDPR:

In accordance with article 83.1 "Each control authority will guarantee that the imposition of

administrative fines under this article for breaches of the

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

effective, proportionate and dissuasive."

Article 83.2 establishes: "Administrative fines will be imposed, depending on the

circumstances of each individual case, in addition to or in lieu of the measures



referred to in article 58, paragraph 2, letters a) to h) and j). When deciding the tax

of an administrative fine and its amount in each individual case will be

due account:

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

nature, scope or purpose of the processing operation in question, as well as

such as the number of interested parties affected and the level of damages that

have suffered;

b) intentionality or negligence in the infraction;

c) any measure taken by the controller or processor to

alleviate the damages and losses suffered by the interested parties;

d) the degree of responsibility of the controller or processor,

taking into account the technical or organizational measures that they have applied under

of articles 25 and 32;

e) any previous infringement committed by the controller or processor;

f) the degree of cooperation with the supervisory authority in order to remedy the

infringement and mitigate the possible adverse effects of the infringement;

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

h) the way in which the supervisory authority became aware of the infringement, in

particular whether the person in charge or the person in charge notified the infringement and, if so, in what

extent;

i) when the measures indicated in article 58, paragraph 2, have been ordered

previously against the person in charge or the person in charge in relation to the

same matter, compliance with said measures;

j) adherence to codes of conduct under article 40 or to mechanisms of

certification approved in accordance with article 42, and

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

such as financial benefits obtained or losses avoided, directly or

indirectly, through the infringement."

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

"Sanctions and corrective measures", provides:

"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."

IX



Determination of the amount of the fine. Violation of article 6.1. GDPR:

Registration of a prepaid mobile line associated with the NIF of the claimant.

Regarding the violation of article 6.1. of the GDPR that has been analyzed in the

Basis V of this resolution, we consider that they concur as aggravating circumstances

the circumstances listed below, which are a manifestation of a

greater unlawfulness of the conduct or greater culpability:

1. Article 83.2.a): the duration of the infringement taking into account the nature,

scope or purpose of the processing operation, as well as the number of interested parties

affected and the level of damages suffered.

The violation of article 6.1 of the GDPR to which we refer participates in the

nature of the so-called permanent infringements, in which their consummation

is projected in time beyond the initial event and extends, violating the

data protection regulations during the entire period of time in which the data

is subject to treatment. Regarding the characterization of the infringements of this

nature have been pronounced, by way of example, the judgments of the Court

National of 09/16/2008 (Rec.488/2006) and of the Supreme Court of 04/17/2002 (Rec.

466/2000)

In this particular case, the infringing conduct began on 11/17/2020, the date on which

that the defendant registered a prepaid line linked to the claimant's NIF, and

terminated the illicit treatment on 05/27/2021, seven months after the start of the

infringement.

VODAFONE has rejected the application of this aggravating circumstance (see Sixth Background,

allegations to the initiation agreement). The reasons on which the defendant bases its

refusal and the reasons why, in his opinion, this aggravating circumstance could not be admitted, are,

in summary, the following:

It argues that the sentences that the AEPD has cited -SAN of 09/16/2008 and of the T.S.

of 04/17/2002- refer to assumptions of fact whose nature is completely

different from the one proposed here and do not deal with the protection of personal data.

staff.

In response to what is alleged, it is enough to indicate that with the aforementioned sentences it has not been

intended to illustrate any specific data protection issue but to corroborate,

through the doctrine of the A.N. and the jurisprudence of the T.S., the concept of infringement

permanent, since the permanent nature of the offense is connected in this case with

its "duration", which is one of the factors to take into account to appreciate the

concurrences of the circumstance of article 83.2.a) of the GDPR.

VODAFONE has also argued that, in accordance with the Sole Additional Provision and the

Article 5 of Law 25/2007, was obliged to treat and preserve "the number

corresponding to the identification document".

Regarding that statement of the defendant, it should be noted that it is disproved

tenor of the exhibition that with respect to the infraction that concerns us is made in the



Legal Foundation V of this resolution, since the treatment carried out was not

protected by the precepts alleged to the contrary.

The defendant has also invoked that, in the present case, there is only one affected person, the

claimant, and that the generation of damages has not been proven.

Ignoring the question of damages, which are evident if we

we look only at the multitude of steps that the claimant has been forced to take

carry out in the event of a violation of your fundamental right to data protection

by VODAFONE, it must be remembered that, according to article 83.2.a) of the GDPR,

The "duration of the infringement" will be assessed taking into account not only the number of

interested parties affected and the damages caused, but also the nature,

scope or purpose of the processing operation in question. and the look

truly relevant with a view to the application of this circumstance is not -as

maintains the defendant - that there is only one affected, but the purpose pursued by the

treatment operation provided for in the Sole Additional Provision of Law 25/2007:

establish instruments to control the use of equipment for criminal purposes

of mobile telephony acquired through the prepaid modality (Preamble of the Law

25/2007).

With regard to VODAFONE's objection that in the matter under examination there is only one

affected -the claimant- should be brought up, since they distort this objection of the

claimed and are applicable to the factual assumption raised, the considerations that,

in relation to article 83.2.a) of the GDPR, make Guidelines 4/2022 of the Committee

European Data Protection Agency (CEPD) for the calculation of administrative fines

pursuant to the GDPR, approved for public consultation on 05/12/2022.

The Guidelines (the original version, in English, deals with this issue in the

paragraph 54 point 4) refer to "the number of specific interested parties, but also

potentially affected

". In this sense, they specify that the greater the number

of stakeholders involved, the more weight may be attributed to this factor by the authority of

control. That, in many cases, it can also be considered that the offense adopts

«systemic» connotations and, therefore, can affect, even in different

moments, to other interested parties who have not submitted claims or reports to

the supervisory authority. That the supervisory authority may, depending on the

circumstances of the case, consider the relationship between the number of interested

affected and the total number of stakeholders in that context (for example, the number of

citizens, customers or employees) in order to assess whether the infringement is of a

systemic and that the greater the number of stakeholders involved, the more weight

The supervisory authority may attribute to this factor.

2. Circumstance of article 83.2.d), "the degree of responsibility of the person responsible or

of the person in charge of the treatment, taking into account the technical or organizational measures

that they have applied by virtue of articles 25 and 32;”

The principle of proactivity provided for in article 5.2. of the GDPR means transferring to the responsible for the treatment the obligation not only to comply with the regulations, but also that of being able to demonstrate its compliance. Among the mechanisms that the GDPR contemplated to achieve this are those provided for in article 25, "protection of data from design”, according to which the controller must apply “both in the



time of determining the means of treatment as at the time of the treatment" technical and organizational measures that guarantee that it makes an effective application of the principles of the RGPD on the occasion of the treatments that it carries out.

The exposition that has been made in this resolution on the protocol that VODAFONE continues to verify that in the processing of personal data carried out in application of Law 25/2007, the principles of data protection are complied with, evidence that it had not applied any measure that meets the provisions of the Article 25 of the GDPR, which is why the existence of the circumstance of the Article 83.2.d) as an aggravating circumstance

The measures that VODAFONE has been applying to comply with the legality principle regarding the personal data that is collected during the contracting of a prepaid card consist solely of the imposition of contractual obligations to those in charge and sub-processors, in particular, the obligation to identify the acquirer of the smart card by means of an original document. No However, even this last requirement was not included in the contract that the distributor

celebrated with the point of sale that has intervened in the contracting,

***ESTABLISHMENT.1.

The defendant has not established any mechanism that allows it to verify that the contractual obligations assumed by subjects such as the distributor and the point of sale are met. VODAFONE has not alleged, let alone proven, that they are measures to verify compliance with these contractual obligations.

It is not necessarily about keeping the copy of the DNI; but the truth is that neither has not even planned to carry out checks through audits or other systems verification of the effective compliance made by the points of sale of the obligations imposed in the contract regarding the identification protocol of the purchaser of prepaid services.

The reality is, as has been exposed when analyzing this infraction, that VODAFONE's security policy consists of taking for granted, by the sole reason that this is stipulated in the contracts, that in the contracting of a smart card, and despite the interest that the point of sale has in closing the transaction, the display of the document is collected from the prepaid card applicant identification, the applicant displays it and the point of sale verifies that the data provided by the client coincide with those that appear in the original document exhibited. Nothing more, since it has not designed measures to verify compliance real and effective that the sub-responsible for treatment of the obligations incorporated into the different contracts

VODAFONE has rejected the application as an aggravating circumstance, article 83.2.d).

The arguments that the defendant has invoked are distorted by the considerations that are made regarding this infraction in Fundament V of this resolution, which corroborate that in no case was it designed, in order to comply

the principles that govern the right to data protection, none of the

measures referred to in article 25 of the GDPR.



3. Circumstance of article 83.2.e) "Any previous infringement committed by the

responsible or in charge of treatment."

In a first approach to this provision of the GDPR that refers to "all

previous infraction" committed, it is appreciated that the norm does not make any delimitation or

delimitation of the set of offenses committed by a person responsible or

person in charge of treatment, either due to the legal nature of the infringement,

by the precept violated, or by the time elapsed since its commission or from the

imposition of the sanction.

However, a systematic interpretation refers us to recital 148 of the GDPR

which includes some guidelines "In order to reinforce the application of the rules of this

Regulation [...]" and indicates in this regard that "However, special attention must be paid to

attention to the nature, seriousness and duration of the infringement, to its nature

intentional [...] or any pertinent infraction [...]".

Recital 148 does introduce a delimitation in the group formed by the

totality of the infractions committed by a person in charge or in charge of

treatment, as it urges special attention to be paid to any "relevant" infringement.

Term that responds to the translation of the adjective "relevant", which appears in the text

original in English, and that means pertinent or relevant.

We believe that, in accordance with section e) of article 83.2. of the GDPR, in the

determination of the amount of the sanction of administrative fine may not fail to

assess all those previous infractions of the person in charge or of the person in charge of

treatment that are pertinent or relevant in order to gauge the unlawfulness of

the conduct being evaluated or the guilt of the offending subject. In addition, a

correct interpretation of the provision of article 83.2.e) GDPR cannot ignore the

purpose pursued by the rule: decide the amount of the fine

administration, in the individual case raised, always considering that the sanction

be proportional, effective and dissuasive.

In this sense, they were cited in the opening agreement and in the resolution proposal, and

again, the resolutions issued by the AEPD in the following

sanctioning procedures processed against the defendant:

i.PS/00193/2021. Resolution issued on September 9, 2021 in which the

a penalty of 40,000 euros. The facts related to the treatment of the NIF of the

claimant without legitimacy linked to the contracting of two mobile lines and a pack

of terminals.

ii.PS/00186/2020. Resolution issued on August 31, 2020 in which the

a penalty of 60,000 euros. The facts related to the treatment of the data

of the claimant without legitimacy linked to the contracting of a fixed line, a line

mobile, internet and television.

iii. PS/00009/2020. Resolution issued on July 28, 2020 imposing a

fine of 48,000 euros. The facts related to the treatment of the data of the

claimant without legitimacy linked to the portability of a number and line registration

made by a third party.

iv. PS/303/2020. Resolution issued on October 26, 2020 imposing a

fine of 36,000 euros. The facts related to the treatment of the data of the

claimant without legitimacy linked to the purchase of a mobile terminal and the registration of

a line with a commitment to stay made by a third party.

v. PS/348/2020. Resolution issued on November 6, 2020 imposing

a fine of 42,000 euros. The facts related to the treatment of the data of the

claimant without legitimacy linked to the portability of a number and line registration

made by a third party

VODAFONE's history of infractions in which there was a significant omission

of the diligence necessary to verify the identity of the person who communicates as data

own the data of a third party, affects the guilt and illegality of the

behavior that we now value.

In the procedures that are related and in the factual assumption that concerns us, the

omission of the appropriate diligence, aimed at identifying the person providing

as your personal data of which you are not the owner, allowed identity fraud

and determined that the defendant processed the personal data of the affected party without

law, violating article 5.1.a) in relation to article 6.1. GDPR.

This history of non-compliance confirms that, when the events occurred in the

that the current violation of article 6.1 is specified. GDPR, the defendant knew

perfectly the deficiencies of its privacy policy to

comply with the obligations imposed by the GDPR in relation to the principle of legality and

the principle of proactivity. The sanctioning resolutions mentioned

should have been an additional reason to review the protocols you have

established to verify the identity of clients on the occasion of contracting

of the products or services that it sells.

VODAFONE opposes the application of this aggravating circumstance. He states that he "disagrees" with what the AEPD has understood by "pertinent antecedents" and adds that the related procedures in the initiation agreement (which were reiterated in the proposal resolution) dealt with cases other than the one at hand, given that in they, the third parties that posed as the claimants, contracted products “through names of the claimants" and the latter received the corresponding invoices, Which hasn't happened now.

However, VODAFONE's allegation regarding the application of this aggravating circumstance must also be rejected. These details are enough:

The first, that, as indicated in relation to this circumstance - section e) of article 83.2 GDPR - the literalness of the precept - "Any previous infringement committed by the person in charge or in charge of the treatment"- is extraordinarily broad and does not makes no comment, so a literal interpretation would have led to frame in it any infringement of the data protection regulations by the that the defendant had been penalized.



The AEPD has interpreted this provision restrictively and has restricted its application limiting it to those infractions that suppose a "preceding pertinent” in relation to the offense being prosecuted. But it is one thing to restrict the scope of the circumstance of article 83.2.e) on the basis of an interpretation systematic of that norm and another very different one what tries VODAFONE. Claim

that it cannot rely on the aforementioned provision.

Judging by their statements, what VODAFONE seeks is that the application of

this circumstance is subordinated to the existence of a "factual identity" of the

infractions; identity between the facts on which the infractions for which

that was sanctioned in the past and the facts that concern us. However, as

has explained, the antecedents that have been mentioned are "pertinent" in a

assumption like the one presented here. In the precedents cited, there had been no

adopted measures aimed at verifying the identity of the person who

contract. Measures to ensure that the processing of personal data was lawful and

that would allow it to demonstrate that it was obliged to adopt in accordance with the articles

5.2, 24 and 25 of the GDPR.

4. Circumstance of article 83.2.g) "the categories of personal data

affected by the infringement.

The RAE dictionary defines the term "category" as "each of the classes or

divisions established when classifying something". Reading article 83.2.g) of the GDPR gives us

refers, initially, -making a literal and strict interpretation of the norm- to the

heading of article 9 of the GDPR, "Treatment of special categories of data

personal data", thus concluding that the GDPR classifies personal data, only,

in specially protected and the rest.

A systematic and teleological interpretation of article 83.2.g) of the GDPR connects this

precept with other classifications offered by the text of the GDPR that, in addition,

respond better to the purpose pursued by the standard: graduating in the individual case the

administrative fine that must be imposed respecting in any case the principles of

proportionality and effectiveness.

In this sense, recitals 51 and 75 of the GDPR distinguish a group of data

personal data that, by their nature, are particularly sensitive because of the

significant risk that they may entail, in the context of their treatment, for

fundamental rights and freedoms. The common denominator of all of them is that their

treatment involves a significant risk to the rights and freedoms

fundamental since it can cause physical, material or

immaterial.

This group or category of particularly sensitive data includes data

specially protected rights regulated by article 9 of the GDPR - recital 51 of the

GDPR- and, in addition, many other data not regulated in that precept. The recital

75 mentions in detail the personal data whose processing may entail a

risk, of variable severity and probability, to the rights and freedoms of

natural persons as a consequence of the fact that they can cause damages

physical, material or immaterial. Among them, he mentions those whose treatment

“may give rise to problems of discrimination, identity theft or fraud,



financial loss, damage to reputation, loss of data confidentiality

subject to professional secrecy, unauthorized reversal of pseudonymization or

any other significant economic or social harm;” (The underlining is ours)

Through the numerical identifier of the DNI together with the verification character

corresponding to the tax identification number, the natural person is identified

unquestionably. This quality of the DNI/NIF number makes it a data

particularly sensitive insofar as, if the processing of this data is not

accompanied by the necessary technical and organizational measures to ensure that

whoever identifies with it is really its owner, a third party can supplant the

identity of a natural person with total ease, or, in other words, it can

cause identity fraud, with the risks that this entails for privacy,

the honor and patrimony of the supplanted.

It is estimated that, in this case, the unlawful treatment that the defendant has carried out falls

on a particularly sensitive piece of information: the DNI/NIF of the claimant. That data, by itself

alone, allowed his identification, which affects the seriousness of the behavior of

VODAFONE must appreciate the concurrence as an aggravating circumstance of the

circumstance of section g) of article 83.2. GDPR.

VODAFONE rejects the application of this aggravating circumstance, justifying that "it has not

there has been an identity theft"; in which the claimant's NIF "was not exposed

by Vodafone, but it appears published in the BOE" and that it was not her, the entity

claimed, who provided the third party with that information, but already had it in their possession.

Also in that case the defendant's arguments must be rejected:

Regarding the allegation that "there has not been an identity theft" it should be noted

that when recital 75 of the GDPR refers to the processing of data

“may give rise to problems of discrimination, identity theft or fraud,” not

You are using the terms usurpation and fraud in a legal technical sense, that is,

as behaviors that meet the requirements to be subsumed in a criminal offense

contemplated in the Spanish Penal Code.

Regarding VODAFONE's statement that there was no usurpation of

identity we understand that with it he is referring to the fact that the type of the

Article 401 of the Spanish Penal Code, which is true. However, the GDPR is a

standard applicable to all Member States of the Union whose legal systems

legal, except for the regulations of the E.U. that links them, they are disparate,

even more so when it comes to criminally typified conducts, for what seems

It is clear that the Community legislature did not use those expressions with the meaning

technical legal that the defendant wants to grant them.

In any case, it is recalled that recital 75 refers to usurpation "or" fraud and

that, as is proven, VODAFONE on several occasions described the conduct

that concerns us, and thus registered it in their systems, as a fraud.

On the other hand, it is irrelevant that the claimant's NIF appeared published in

the BOE, since this treatment had its legal basis in the need to comply with a

mission in the public interest or in the exercise of public powers. The publication in the



BOE of the claimant's data for that specific purpose does not legitimize the

subsequent processing of that data by the third party that contracted with VODAFONE,

nor even less can it justify the treatment carried out by the defendant herself.

5. Circumstance of article 83.2.k) GDPR in relation to article 76.2.b)

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

processing of personal data.

The defendant, in the development of its own activity, needs to treat

customary data of a personal nature and this fact affects the diligence that results

required in compliance with the principles that govern the processing of personal data.

personal character and on the quality and effectiveness of the technical and organizational measures

that must be implemented to guarantee respect for this right

of both its clients and third parties.

Extenuating circumstances that VODAFONE invokes:

The mitigations whose application is requested regarding this infraction are:

(i) The "absence of intentionality or negligence", article 83.2 b) of the GDPR.

(ii) the "cooperation with the supervisory authority in responding to the transfer of the claim and having provided the requested information", article 83.2 f) of the GDPR.

None of the mitigations invoked can be admitted.

(i) Regarding the alleged non-existence of intentionality or negligence, we refer to the considerations made in Fundamental V about the concurrence of the element of guilt, materialized in a serious lack of diligence.

(ii) Regarding the second mitigation, it is indicated that article 83.2.f) of the GDPR is refers to the "degree of cooperation with the supervisory authority in order to put remedy the breach and mitigate the potential adverse effects of the breach;" (he underlining is ours) and the response of the defendant to the information requirement of the Inspection Sub-directorate did not meet these purposes, so it is not framed in that mitigation.

In view of the foregoing, it is agreed to impose VODAFONE for the infringement of article 6.1. of the GDPR, typified in article 83.5.a), specified in having given registration of a prepaid line associated with the NIF of the claimant, a fine of €70,000.

X

Determination of the amount of the fine. Infringement of article 17 of the GDPR:

Regarding the conduct contrary to the RGPD that has been analyzed in the Foundation VII of this resolution, the concurrence of the following circumstances that affect the liability payable to the claimant and that are a manifestation of a greater illegality of his conduct or greater guilt:

1.Article 83.2.a): It has special relevance, and, therefore, the consequent reflection in the amount of the fine to be imposed, the seriousness of the conduct in which

this infraction is specified in attention to the nature and purpose of the operation of

treatment.

In the case examined, the "nature" of the operation is especially relevant.

of treatment because, due to the conduct of VODAFONE, the claimant has been

without legal basis of one of the mechanisms that the RGPD grants you to

make effective and guarantee your right to the protection of personal data. fits

add that the defendant repeated her conduct despite the fact that she had elements of

judgment more than sufficient to qualify the treatment of personal data of the

claimant linked to the registration of the prepaid line as a fraud, which forced him to

proceed to delete the data. Despite being aware of this circumstance, he deprived the

claimant of the right granted by the GDPR and the response to deny the right

did not take into account the provisions of Article 17 of the GDPR as it claimed

as reason, exclusively, technical reasons related to the impossibility of

cancel a prepaid line that in no way justify the refusal.

The foregoing considerations on the "nature" of the violation of Article 17

of the GDPR for which VODAFONE is held responsible are in line with the

criterion that follows the Guidelines 4/2022, on the calculation of fines

pursuant to the GDPR, prepared by the CEPD and approved for its

public consultation. Paragraph 54.a) of the original English version indicates that

respect that the supervisory authority may review the interest that the provision

infringed purports to protect and the place that provision occupies in the legal framework

of the protection of personal data. In addition, the supervisory authority may take into account

account the degree to which the infringement has impeded the effective application of the disposition and the fulfillment of the objective that it was intended to protect.

The "purpose" of the processing operation, which affects the severity of the infringement, is connected to VODAFONE's response in which it denied the claimant the right of deletion; response that he reiterated and that was clear contradiction with article 17 of the RGPD and that was issued by the department of data protection of the operator, to whose email address the claimant addressed your deletion request. To this same address and department should be addressed the VODAFONE customers, which is at the time the largest telephone operator in the country by the number of clients, since it provides service to more than twenty percent of the domestic market users. This demonstrates the scope of the behavior of VODAFONE in which the alleged infringement materializes, it being irrelevant that the claimant has been a single person.

VODAFONE rejects the application of this aggravating circumstance of article 83.2.a) of the GDPR and says:

"The Agency blames Vodafone for an "absolute ignorance of the content of the right" of suppression, ignoring, in the opinion of this Agency, "what are the obligations that derive for it from article 17 of the GDPR".

That being said, with all due respect, we disagree with the character generalized subjective assessment of the Agency. As we have shown in the Fifth Allegation, to which we refer, although the Agency ends understanding that Vodafone has infringed article 17 of the GDPR, there are arguments to defend that it has acted in accordance with the provisions in article 17 of the GDPR:

a) You have not treated the DNI number illegally.

b) In any case, it was obliged by law to keep said data and, in addition,

it was necessary for the formulation, exercise or defense of

claims."

The arguments put forward by VODAFONE are in line with the refusal of the

entity to recognize that the treatment of the NIF of the claimant linked to the registration of the

prepaid line was illegal. We refer to the considerations included in the

Basis V of this resolution regarding the violation of article 6.1 by the

Registration of the prepaid line linked to the NIF of the affected party.

About the obligation alleged by VODAFONE to keep personal data

treated within the framework of Law 25/2007 in accordance with its article 5, we must reiterate what

exposed in Fundament V, in the sense that all the treatments that are

carried out under the aforementioned law must respect the regulations for the protection of

data. Thus, in no case could the defendant be bound by virtue of the

Article 5 of Law 25/2007 to keep personal data whose treatment entails

a breach of the GDPR. But, what's more, article 9 of Law 25/2007 says

expressly that the data controller will deny the exercise

of the right of cancellation in the terms and conditions provided in the GDPR, which

which directly refers us to article 17.1 of the GDPR.

2. Article 83.2.b): "intentionality or negligence in the offence". It is outside of

doubt the very serious lack of diligence of the defendant, who did not comply with the deletion

of the NIF data requested by the claimant despite being obliged to do so in accordance with the

article 17.1.d) GDPR.

We are facing a very serious lack of diligence and this is demonstrated by the fact that VODAFONE would have denied the suppression of the NIF on the two occasions that the claimant requested it. requested, despite the fact that the deletion was appropriate in light of the provision of article 17 of the GDPR and that the operator was fully aware then that the personal data of the defendant had been used in a fraudulent contracting.

The arguments with which VODAFONE justified its decision to reject the deletion of the NIF data -exposed in the letters that he addressed to the claimant on 01/26/2021 and 02/03/2021 and that he reiterated, months later, in the letter addressed to the AEPD in July 2021 in response to the information request prior to the admission for processing of the claim - reveal a total ignorance of the applicable regulations -particularly of the GDPR and Law 25/2007- and therefore an absolute lack of diligence in the compliance with the obligations imposed by the GDPR.

VODAFONE rejects the application of this aggravating circumstance and alleges in such sense:

"The Agency describes Vodafone's lack of diligence as "very serious" for not having responded to "the deletion of the NIF data requested by the claimant despite be obliged to do so in accordance with article 17.1 d) GDPR".

Although it is considered that the treatment of the DNI number provided by the third party is unlawful (quod non), the obligation to



conservation imposed by Law 25/2007 which, in the opinion of this party, makes that the infringement cannot be classified as "gross negligence".

In response to this allegation, we refer to the consideration made in point 1

precedent: in essence, that the data processing carried out under the Law

25/2007 is subject to data protection regulations and that article 9 of that

law refers to article 17 of the GDPR.

3.Article 83.2.k) GDPR in relation to article 76.2.b) LOPDGDD: The obvious

link between the business activity of the defendant and data processing

personal, both clients and third parties, required him to have implemented the

adequate measures to correctly address the subjective rights that the GDPR

granted in articles 15 to 22.

Attention to the right of deletion (article 17) requires that the response that the

claimed offer is adjusted to law. Failure to comply with the obligations

derive for it from article 17 is especially serious if it is assessed that we are facing

an entity for which the treatment of

Personal data. Especially if the number of customers is taken into account.

Attenuating. VODAFONE requests that the following circumstances be appreciated

mitigating:

(i) "cooperation with the supervisory authority in responding to the transfer of the

claim and having provided the requested information", article 83.2 f) of the GDPR.

(ii) The "absence of benefits obtained through the infringement", article 83.2 k)

of the GDPR and 76.2 c) of the LOPDGDD.

None of the mitigations invoked can be admitted.

(i) Article 83.2.f) of the GDPR refers to the "degree of cooperation with the authority of

control in order to remedy the infringement and mitigate the possible effects

adverse effects of the offence;". The respondent's response to the information request

of the Sub-directorate of Inspection did not meet these purposes, so it is not

framed in that mitigation.

(ii) On the application of article 76.2.c) of the LOPDGDD, in connection with article

83.2.k), non-existence of benefits obtained, it should be noted that such circumstance only

it can operate as an aggravating circumstance and in no case as a mitigation.

Article 83.2.k) of the GDPR refers to "any other aggravating or mitigating factor

applicable to the circumstances of the case, such as the financial benefits obtained or the

losses avoided, directly or indirectly, through the breach." and the article

76.2c) of the LOPDGDD says that "2. In accordance with the provisions of article 83.2.k) of the

Regulation (EU) 2016/679 may also be taken into account: [..] c) The benefits

obtained as a consequence of the commission of the infraction." Both provisions

mentioned as a factor that can be taken into account in grading the sanction

the "benefits" obtained, but not the "absence" of these, which is what VODAFONE

alleges.



In addition, in accordance with article 83.1 of the GDPR, the imposition of fine sanctions

is governed by the following principles: they must be individualized for each

particular case, be effective, proportionate and dissuasive. The admission that it operates

as a mitigation, the absence of benefits is contrary to the spirit of article 83.1

of the GDPR and the principles governing the determination of the amount of the

fine penalty. If, as a result of the commission of a violation of the GDPR, it is classified as

mitigating the non-existence of benefits, partially annuls the dissuasive purpose that

complies through sanction. Even more so when, as occurs with the infringement of the

Article 17 of the GDPR at hand, we are dealing with infringing conduct that does not

has no relationship of any kind with obtaining profits, so there would be no

no connection between the mitigation applied and the circumstances surrounding

the infringing conduct, so that the absence of benefits could not be an exponent

of greater or less illegality or guilt. Accept the VODAFONE thesis

In a case like the one at hand, it would mean introducing an artificial reduction in the

sanction that truly proceeds to be imposed; which results from applying the

circumstances of article 83.2 GDPR that must be assessed.

The Administrative Litigation Chamber of the National Court has warned that the

fact that in a specific case not all the elements that

constitute a circumstance modifying liability that, by its nature,

has an aggravating nature, cannot lead to the conclusion that said circumstance is applicable

as a mitigation. The pronouncement made by the National Court in its

SAN of 05/05/2021 (Rec. 1437/2020) -even though that resolution is seen on the

circumstance of section e) of article 83.2. of the GDPR, the commission of infringements

above- can be extrapolated to the question raised, the claim of the defendant of

that the "absence" of benefits be accepted as mitigating, being that both the

GDPR and LOPDGDD refer only to "the benefits obtained":

"Considers, on the other hand, that the non-commission should be considered as mitigating

from a previous violation. Well, article 83.2 of the GDPR establishes that

must be taken into account for the imposition of the administrative fine, among

others, the circumstance "e) any previous infringement committed by the person responsible or

the person in charge of the treatment". This is an aggravating circumstance, the fact

The fact that the budget for its application does not meet implies that it cannot be

taken into consideration, but does not imply or allow, as the plaintiff claims,

its application as a mitigation";

In view of the foregoing, it is agreed to impose on the defendant for the infringement

of article 17 of the GDPR, typified in its article 83.5.b), an administrative fine for

an amount of €100,000.

Therefore, in accordance with the applicable legislation and assessed the criteria of

graduation of sanctions whose existence has been accredited,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: DECLARING the termination of the disciplinary procedure regarding the

violation of article 15 of the GDPR, in accordance with the provisions of article

85 of the LPACAP.



SECOND: Regarding the infringement of article 6.1 of the GDPR derived from having

treated without legal basis the NIF of the claimant to consult a solvency file,

AGREE on the FILE of the open disciplinary procedure against VODAFONE

ESPAÑA, S.A.U., with NIF A80907397, having been accredited in the file

that it is not responsible for that infringing conduct that was attributed to it in the agreement of

initiation of this procedure, PS/00281/2021.

THIRD: IMPOSE VODAFONE ESPAÑA, S.A.U., with NIF A80907397, for a

violation of article 6.1. of the GDPR, typified in article 83.5.a) of the GDPR,

materialized in having registered a prepaid line associated with the NIF of the claimant,

an administrative fine of €70,000 (seventy thousand euros).

FOURTH: IMPOSE VODAFONE ESPAÑA, S.A.U., with NIF A80907397, for a

infringement of article 17 of the GDPR typified in article 83.5.b) of the GDPR, a

administrative fine of €100,000 (one hundred thousand euros).

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

SIXTH: Warn the sanctioned entity that it must make the sanction effective

imposed once this resolution is enforceable, in accordance with the

provided in art. 98.1.b) of Law 39/2015, of October 1, on Procedure

Common Administrative Office of Public Administrations (hereinafter LPACAP), in the

voluntary payment term established in art. 68 of the General Regulation of

Collection, approved by Royal Decree 939/2005, of July 29, in relation to the

art. 62 of Law 58/2003, of December 17, by entering it, indicating the NIF

of the sanctioned party and the number of the procedure that appears in the heading of this

document, in the restricted account number ES00 0000 0000 0000 0000 0000, open to

name of the Spanish Data Protection Agency in the bank

CAIXABANK, S.A. Otherwise, it will be collected in the period

executive.

Once the notification has been received and once executed, if the execution date is

between the 1st and 15th of each month, both inclusive, the term to make the payment

voluntary will be until the 20th day of the following or immediately following business month, and if

between the 16th and the last day of each month, both inclusive, the payment term

It will be until the 5th of the second following or immediately following business month.

In accordance with the provisions of article 50 of the LOPDGDD, this

Resolution will be made public once the interested parties have been notified.

Against this resolution, which puts an end to the administrative process in accordance with art. 48.6 of the

LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the

Interested parties may optionally file an appeal for reversal before the

Director of the Spanish Agency for Data Protection within a period of one month from

count from the day following the notification of this resolution or directly

contentious-administrative appeal before the Contentious-administrative Chamber of the

National Court, in accordance with the provisions of article 25 and section 5 of

the fourth additional provision of Law 29/1998, of July 13, regulating the

Contentious-administrative jurisdiction, within a period of two months from the



day following the notification of this act, as provided for in article 46.1 of the

referred Law.

Finally, it is noted that in accordance with the provisions of art. 90.3 a) of the LPACAP,

may provisionally suspend the firm resolution in administrative proceedings if the

The interested party expresses his intention to file a contentious-administrative appeal.

If this is the case, the interested party must formally communicate this fact through

writing addressed to the Spanish Data Protection Agency, presenting it through

of the Electronic Registry of the Agency [https://sedeagpd.gob.es/sede-electronica-

web/], or through any of the other registries provided for in art. 16.4 of the

aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the

documentation proving the effective filing of the contentious appeal-

administrative. If the Agency was not aware of the filing of the appeal

contentious-administrative proceedings within a period of two months from the day following the

Notification of this resolution would terminate the precautionary suspension.

Mar Spain Marti

Director of the Spanish Data Protection Agency

938-120722

28001 – Madrid

www.aepd.es

sedeagpd.gob.es