 File No.: PS/00340/2021

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 claimant) files a claim with the

Spanish Data Protection Agency (AEPD) dated 03/04/2021. The

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

forward, VODAFONE or the claimed party).

The claim is based on the following facts: the defendant registered a line

prepaid phone number ***TELEPHONE.1, linked to the personal data of the

claimant and transferred their data associated with said line to the Civil Guard of

***LOCATION.1,

“and/or Mixed Court number 5 of

***LOCATION.3 and Court number 1 of ***LOCATION.4”. The claimant

states that she has been summoned by both courts as being investigated by the

scams committed through Wallapop by the telephone line that VODAFONE

linked to his person.

***LOCATION.2

SECOND: Before addressing the AEPD, the claimant submitted to the

Secretary of State for Telecommunications and Digital Infrastructures (SETID), with

dated 11/04/2020, a claim against VODAFONE for the registration of the line

phone number ***TELEPHONE.1 (hereinafter, the disputed line) without your

consent and for violating your personal data. The claimant mentions the

existing discrepancy between the information that VODAFONE provided to the Civil Guard -

provided the claimant's data contained in its systems associated with

the disputed line - and the one provided to SETID, according to which the claimant did not

was listed in their systems as a customer and was not, nor had been, the owner of the line

prepayment object of the claim.

In the course of the file processed before the SETID -with the reference

***REFERENCE.1- VODAFONE issued a report stating that, regarding the

disputed line, the claimant was not a client of his, and therefore did not have any

active service, and added that this mobile line did not belong and did not belong then to the

claimant, reason for which he could not attach the contract associated with the line that was

he had requested. The SETID issued a resolution on 03/04/2021 in which it agreed to estimate

the claim in relation to the unsolicited discharge, recognizing the right of the

claimant to obtain immediate cancellation of the service and not to pay the invoices that

could have issued the operator.

The claimant has provided an annex to her claim, in addition to the resolution issued

by SETID and the response that the defendant addressed to the Secretary of State on

11/25/2020, the following documents that come from the Civil Guard, post of

***LOCATION.2.



(i) Document with the title "Procedure to attach documents", which includes

that, being 03/24/2020, "it is stated that the following are attached

documents: Preliminary Proceedings XX/XXXX for fraud over the Internet with

identified".

(ii) Document that bears the handwritten indication "folio 11" in which this information:

“Vodafone (...). Court: Judicial Police; Criminal Procedure: Preliminary Investigations XX/XXXX; Reception date: 03/10/20; Response date: 03/10/20; Query type: LC.01 Holder by MSISDN and range of dates; Target: ***PHONE.1; Period of Search: from 2020-02-12T00:00:00 Europe/Madrid to 2020-0306T23:59:59 Europe/Madrid; Records:1”. Immediately below it is: “Name: [the name of the claimant]; Last name:

[both surnames of the claimant]; Document: ***REFERENCE.2; Document Type: AR-PASSPORT; Line: ***PHONE.1; Guy Contract: PREP; Added Date: 11/29/2019”.

(iii) "Procedure consigning identification of a person":

"In ***LOCATION.2, being (...) March 24, 2020, by this Diligence certifies that, as a consequence of the steps taken, they have obtained the identification data of the person indicated below whose data are:

Name: [name and two surnames of the claimant] (DNI ***NIF.1).

[...]

Date of Birth: 04-24-198j

Father's name: B.B.B.

Mother name: C.C.C

Address: ***ADDRESS.1.

It is stated that the identification was made by answering VODAFONE as the owner of the phone number ***TELEFONO.1, quoted by the complainant.

The person identified in this proceeding is aware of another address in Base de DGT data, being the following: ***ADDRESS.2 [...]” (The underlining is ours)

THIRD: Transfer of the claim and information of the claimant prior to the admission to processing of the claim formulated.

In accordance with article 65.4 of Organic Law 3/2018, of December 5, of Protection of Personal Data and guarantee of digital rights (hereinafter LOPDGDD), said claim was forwarded to VODAFONE so that it could proceed to its analysis and inform this Agency within a month of the actions carried out to adapt their actions to the data protection regulations.

The letter was served electronically to the claimed party who agrees to the notification on 04/12/2021, as stated in the certificate issued by the Support of the Electronic Notification Service and Authorized Electronic Address of the National Currency and Stamp Factory (hereinafter, FNMT).

The defendant did not respond to the information request until 07/16/2021, after more than three months since you had access to the notice. In her response, the Claimant states the following:



1. That, after the appropriate investigations, it has sent a letter to the claimant informing you of the steps taken to resolve the claim and apologizing for the inconvenience caused. Attach as document 1 the copy of the letter dated 06/28/2021 in which it says, among other things:

"(...) we want to inform you that we have been able to verify that the telephone line ***TELEPHONE 1

had registered in our systems with their data and, among

others, with a passport number. As a consequence, when the Secretary of

State of Telecommunications and Digital Infrastructures sends us your

claim and search our systems with the information from which

We have your ID, it does not appear that you are the owner of the aforementioned line. In

On the other hand, when the Civil Guard asks us for ownership of the line, it appears that it is

registered with your name and with a passport number, information that was

provided to the Civil Guard. This use of your data has led to the communication

your data to the Civil Guard, this institution being the one that has the means to

corroborate if the information provided, your name and passport number, were the

correct with respect to his person."

(The underlining is ours)

Provide as document 2 the letter that he sent you on 03/17/2021, sent "in

compliance with the estimated resolution in your favor, with file number

***REFERENCE.1", which included this relevant information for the purposes that we

occupy: "We wish to inform you that, as established in said resolution, the

***TELEPHONE 1

line

and to this day there are no

service on your behalf."

has already been disconnected

2.Regarding the causes that led to the incident, the defendant explains that the

The claim is caused by an action of the Civil Guard of ***LOCATION.2 in the

. And says

who requested information on the ownership of the telephone line

that, "Given this request, it proceeds to provide the information it had in its systems,

appearing the prepaid line in the name of [name and two surnames of the

claimant], with passport number ***REFERENCE.2.”

controversial

Provide as document 3 "the services registered with the passport" indicated. He

Document 3 is made up of two screenshots that correspond to the

“Customer Interaction Manager” page. In it, in the box dedicated to

"Caller Information", in the "customer" tab, the name and both surnames appear

of the claimant. In the "Central Information Page" box, in one of the two

screenshots show the "Date of registration" tab, field that is empty; In the

Another screenshot shows the "NIF/NIE/Passport/CIF" tab and this information:

***REFERENCE.2.

The defendant adds with regard to the report that she sent to the SETID, in which she

certify that the claimant was not a client of the company and that she did not have any credit lines

active, that "This information is from our systems since the

searches are carried out by tax identification number (DNI/NIF), so the

It was carried out with the claimant's DNI, ***NIF.1, verifying that it was not

there are active services. As a consequence, the SETID upholds the claim of the

Mrs. [the claimant], it being necessary to carry out the immediate withdrawal from the

the line ***TELEPHONE.1 that was registered under another identification number



(Passport ***REFERENCE.2) under the name of the claimant. This process is

carried out, as indicated in Document number 2 of the manifestation

second of these allegations.

Regarding the inconsistency between what was stated before the SETID and the information that

provided to the Civil Guard to which the claimant refers, indicates that the root of the problem

“It is fraud carried out by a third party. In other words, when the Civil Guard requests the

phone information ***TELEPHONE.1, the data of the owner appears under the

passport number ***REFERENCE.2. However, when the SETID requests

information on Mrs. [the claimant], is sought with the information available

available, that is, the DNI ***NIF.1, appearing in the Vodafone systems the

services that, at the time, were contracted by the legitimating claimant and with their data, being

all of them unsubscribed and the line ***TELEPHONE.1 is not found among them.”

He insists that this situation "has been the result of the fraudulent use of data from

Ms. [complainant] and the lack of review by the Civil Guard of the

information provided by my client given that a number of

passport that was not contrasted with the national identification bases of the

citizens.”

It says that "This fraud has generated that in the systems of my represented

registered a prepaid line in the claimant's name using a passport

invalid. In this case, security measures were implemented from Vodafone

necessary and the third party that committed the fraud exceeded the Security Policy to

Private Clients, providing the information of the interested party that would have been obtained

by illegal or fraudulent means.

(The underlining is ours)

He states that document number 4, a copy of which he provides, includes the Privacy Policy

Security for Private Clients. This is the "Wholesale Distribution Agreement

prepaid. Non-exclusive to Vodafone” entered into between the operator and the Distributor

Wholesaler CSQ NON STOP SHOP, S.L.,

3. Regarding the measures adopted to prevent "incidents from occurring

similar, dates of implementation and controls carried out to verify its effectiveness",

responds that these measures consisted of disconnecting the disputed line, which

had been registered with information that the claimant does not recognize and notify by

letter to the claimant the actions carried out.

FOURTH: Agreement to open the disciplinary procedure.

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

disciplinary action against the claimed party in accordance with the provisions of articles 63 and 64 of

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

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

Article 6.1 of the GDPR, typified in Article 83.5.a) of the GDPR.

FIFTH: Allegations to the initiation agreement.



Notified the start agreement on 02/04/2022 in accordance with the provisions of the LPACAP,

VODAFONE accepts the notification on 02/07/2022.

In a brief filed on 02/14/2022, the claimed party requests that the term be extended

initially set to present arguments and that a copy be delivered to him

of the file. The claim is responded to in writing dated 02/21/2022 in which

it is agreed to extend the term by the maximum legally permitted and a

copy of the administrative file.

VODAFONE presents its allegations on 02/28/2022. Request, first of all, the

archive of the procedure for understanding that his conduct does not constitute a

infringement of article 6.1 of the GDPR. Subsidiarily with respect to the claim

above, requests the filing of the disciplinary file due to the non-existence of the element

of guilt, which would prevent this Agency from imposing a sanction.

Subsidiarily with respect to the previous claims, that the sanction that is

imposed is set at its minimum amount in attention to the extenuating circumstances whose concurrence

invoke.

In defense of its petitions, it alleges the following:

1.Relates through eleven points the facts that, in his opinion, delimit the object of the

debate:

Yo. They deal exclusively with one person, the claimant, who is also not a customer

from VODAFONE.

ii. On 11/28/2019 "allegedly a third party" requested the registration of a card

prepaid in the name of the claimant, "because she registered" with the name and surname of

the claimant and the passport number ***REFERENCE.2.

iii. The line ***TELEPHONE.1 was registered, which "was allegedly used" by a

third to commit a scam on Wallapop.

iv. On 03/10/2020 the Civil Guard (Police Investigations No. XX/XXXX), sends a

court order to VODAFONE requesting that they be "assigned to this

Unit the following data: Ownership of the subscriber number ***TELEPHONE.1 to

dated February 12, 2020".

v. VODAFONE responds to the Civil Guard on 03/13/2020 informing that the owner of

the line was the claimant and providing the passport information that was obtained from the third party that

contract.

saw. That, "As stated in Annex 2 of the Claim", on 03/24/2020, the

Civil Guard of ***LOCALIDAD.2 issued an identification Diligence, in which

indicates that "as a consequence of the procedures carried out, the

identification data" of the Claimant, which is identified by DNI ***NIF.1."

vii. The claimant filed a claim with the Secretary of State for

Telecommunications and Digital Infrastructures (SETID) on 11/04/2020 in which

states that Vodafone would have registered a line without their consent.

viii. The SETID forwarded the claim to VODAFONE on 11/25/2020, which answers that

"Once the appropriate verifications have been carried out and the facts described have been analyzed

A.A.A., we inform you in reference to the registration of mobile line

by Mrs.

***TELEPHONE.1 unrecognized, which as of the date of this writing, November 25,

2020, Ms. A.A.A. She is not a Vodafone customer, so she does not have any service

active in our Company, and the mobile line ***TELEPHONE.1 does not belong to or



belonged to Ms. A.A.A.". "As Vodafone stated in its Answer to the

Information Requirement, the search was carried out with the DNI of the Claimant,

that was involved in the claim filed with the SETID, which was reported to

Vodafone. The search, carried out by the Claimant's DNI, yielded a result

negative."

ix. On 03/04/2020, the SETID issued a resolution (attached as Annex 3 of the

Claim) in which it orders Vodafone to terminate the claimant from the service

required.

x. On 03/04/2021, the claimant files a claim with the AEPD and on 04/08/2021 the

AEPD sends VODAFONE an information request to which the

06/24/2021.

xi. An agreement is issued to start a disciplinary file against VODAFONE for violation of article 6.1 of the GDPR "and this because Vodafone would have treated" the personal data of the claimant linked to a prepaid telephone line that she denies having contracted" and Vodafone would not have "contributed with its response to the request for information prior to the admission of this claim for processing, no document or probative element that proves the legal basis of the treatment carried out".

2. She denies having infringed article 6.1 of the GDPR and states that she was entitled to treat the "personal data provided when registering the prepaid card", "between them the passport number provided."

It considers that the treatment carried out has two possible legal bases: Section b) of article 6.1 of the GDPR, "the data provided was necessary to execute the contract", and article 6.1 c) of the GDPR, compliance with a legal obligation in connection with the Sole Additional Provision of Law 25/2007, of October 18, on conservation of data related to electronic communications and networks public communications (hereinafter, Law 25/2007), precept that establishes:

"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".

He concludes his argument by saying that "it is obliged by Law 25/2007 to treat the

"name and surname of the buyer", as well as the "number corresponding to the

identification document used" by the buyer of the prepaid card." (The

underlined is from VODAFONE)



He adds that a "different issue is that said data turns out to be wrong, but this

may not suppose, in any case, a violation of article 6.1 of the GDPR."

3. Secondarily, it alleges the absence of guilt, so even if the

AEPD understands that it has violated article 6.1 of the GDPR, it would not be appropriate to impose

no sanction since there is no guilt in his conduct, neither by fraud nor

by way of guilt

To this end, it cites article 28 of Law 40/2015, of October 1, on the Legal Regime of

Public Sector (hereinafter LRJSP) that regulates the principle of guilt. alludes to the

interpretation made by the Supreme Court: "among others, the Judgment of the Court

Supreme Court of January 23, 1998 [RJ 1998\601]" according to which "for the

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

that the diligence that was required by the person claiming its non-existence has been used."

He mentions the criterion followed by the National Court which, he says, has understood in cases in which a third party has accessed data through criminal activities of the interested parties guarded by a person in charge of the treatment "(it is not the case, Vodafone was not in custody of the Complainant's data)", "that imputing such facts to the responsible for the treatment could lead to the violation of the principle of culpability." It refers to the SAN, (Contentious-Administrative Chamber, Section 1) of 02/25/2010 which indicates:

Thus, even though article 9 of the LOPD establishes an obligation to result, consisting of adopting the necessary measures to prevent the data is lost, misplaced or ends up in the hands of third parties, such obligation does not it is absolute and cannot cover an assumption such as the one analyzed. In the case of records, the result is the consequence of an intrusion activity, not covered by legal system and in this sense illegal, from a third party with high computer technical knowledge than breaking security systems established accesses the database of users registered in www.portalatino.com, downloading a copy of it. And such facts cannot be attributed to the appellant entity, otherwise it would violate the principle of guilt".

The defendant concludes that we are "facing a criminal practice carried out by a third party who, acting fraudulently, has impersonated the Claimant's identity when requesting the registration of a prepaid card on behalf of the Claimant, exceeding the controls established by Vodafone."

Regarding the diligence that was required to identify the applicant for the card prepaid, considers that "the diligence parameter required of Vodafone and the rest of operators" should be "what is required by law".

The legislation that you believe constitutes the due diligence measure is, for

On the one hand, Law 25/2007 which, he warns, "does not oblige a copy of the DNI to be kept, but only of the data that appears in the document provided." On the other hand, the Organic Law 5/1985, of June 19, of the General Electoral Regime, on which it comments that, although "it is not applicable to the case, it does serve us as a sample button in order to



to demonstrate that the display of a DNI is sufficient to identify the person who is going to exercise one of the fundamental rights par excellence, the right to vote."

In short, it affirms that it has complied with the provisions of Law 25/2007 and has Appropriate measures have been taken to identify the applicant for the prepaid card. denies that the measures it adopted had been ineffective or insufficient, as maintained by the startup agreement. Regarding the measures implemented, he states:

-That he transferred the obligation of identification to the wholesaler with whom he contracted, CSQ Non Stop Shop, S.L. (CSQ). Provide as document number 3 a screenshot certifying that CSQ contracted with the point of sale in charge of registering the prepaid card of which this claim is the cause, D.D.D. (hereinafter the Point of Sale or D.D.D.)

-That in the first clause of Annex II of the contract signed with the wholesaler CSQ (provided as document number 4), it undertakes to transfer to the point of sale the "essential obligation to identify PRESENTIALLY the Client/Buyer through their original identification card", and it is specified that the Documentation to be presented by natural persons consists of the DNI or NIF or the

Passport or NIE.

He affirms that the events occurred due to human error. It says in this sense that

“[...], the fact of processing personal data that belonged to the Claimant has been

due to the existence of human error, which are unavoidable and on which

Vodafone cannot have effective control. [...], there may be cases, such as the

present, in which Vodafone processes personal data that does not belong to the applicant

of 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.”

He comments that the AEPD has ruled on numerous occasions about the errors

humans, stressing that they cannot be punished. He quotes the SAN of 12/23/2013:

"The question, therefore, must be resolved in accordance with the principles of the

punitive law since mere human error cannot give rise, by itself, to

itself (and especially when it occurs in isolation), to the attribution of

sanctioning consequences; because, to do so, it would be incurred in a system

of strict liability prohibited by our constitutional order".

Finally, we reproduce the comments of the defendant regarding the

considerations included in the agreement to start the procedure:

“[...] in its Commencement Agreement, the Agency would be demanding Vodafone and, therefore,

extension to thousands of Vodafone points of sale and other telephone operators

telephony, that measures be implemented, such as, for example, a software of

scanning and verification of IDs and passports.

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.

That said, if the Agency intends to modify those requirements and increase the

identification requirements to such extremes, in no case may

Vodafone can be accused of negligence or lack of solidity of the measures

taken at this time, but first the rules should be established and

subsequently, where appropriate, penalize the operator that does not apply them, but does

that is not in accordance with the law is to try to use the route directly

penalty as a method of setting security parameters

enforceable." (The underlining is ours)

4. Requests a reduction of the sanction based on the mitigation that invokes and opposes

the admission of the aggravating factors established in the agreement to open the procedure.

Regarding the aggravating circumstances appreciated by the VODAFONE Agency, it makes these

considerations:

-Article 83.2.a) GDPR. The initiation agreement admitted this circumstance as

aggravating factor considering two factors: (i) The seriousness of the infringement taking into account

the level of damages suffered, to the extent that the personal data of

the claimant were linked to the commission of criminal offences. and (ii) the

duration of the infringement, taking into account the purpose of the operation of the

treatment, since the infraction would have started on 11/29/2019 (when he was discharged

line) and the illicit treatment would have ended on 03/17/2021.

The defendant rejects its admission and alleges these reasons:

1. Law 25/2007, in its Sole Additional provision in relation to its article 5,

imposes on VODAFONE the obligation to collect and keep "the name, surnames and nationality of the buyer, as well as the number corresponding to the document identifier used [...]".

2. Article 83.2.a) establishes that the "duration of the offence" will be used as aggravating or mitigating "taking into account the nature, scope or purpose of the processing operation in question as well as the number of data subjects affected and the level of damages they have suffered". However, in the present case, there is only one person affected (the claimant).

3. The Judgments of the National Court of 09/16/2008 (Rec. 488/2006) and of the Supreme Court of 04/17/2002 (Appeal 466/2000) cited in the initiation agreement are not applicable, since the factual assumptions and their nature are completely different. In both judgments, which do not deal with the protection of personal data, we are facing a repeated, conscious and active behavior on the part of the offenders, elements that we did not find in the case of Vodafone.

-Article 83.2.d) GDPR: The degree of responsibility of the controller or manager of the treatment, taking into account the technical or organizational measures that have applied under articles 25 and 32.

The defendant rejects its admission as an aggravating circumstance and alleges these reasons:

The Agency affirms that "it is unknown what organizational measures the implemented and if these were correct and necessary taking into account the current technical development and the evident risk that the contracting of the services that the

claimed entity markets represents for the rights and freedoms of

people"." He answers this question by referring to the first allegation of his

pleadings and says that "in relation to the suitability of requesting the DNI or the

Passport to prove the identity of the applicant. In any case, and as

As we have pointed out, the Initiation Agreement is related to the alleged infringement of article

6.1 of the GDPR, not to the security measures adopted by Vodafone."

-Article 83.2.e) GDPR: "Any previous infringement committed by the person in charge or the

treatment manager".

It rejects its admission as an aggravating circumstance and alleges these reasons:

"The Agency understands that the events that occurred in the

following disciplinary procedures:

PS/00186/2020,

PS/00009/2020, PS/303/2020 and PS 348/2020. We do not agree: if they are reviewed

the factual background of each of these proceedings will be seen that all

they deal with cases in which a third party, posing as the claimants,

has contracted products on behalf of the claimants and the latter have received the

corresponding invoices, which has not happened in the present case, since it is

of a prepaid line.

For the rest, PS/00186/2020 has nothing to do with impersonation of

identity, but with a computer error in the Vodafone systems."

PS/00193/2021,

-Article 83.2.g) GDPR: "The categories of personal data affected

for the offence."

It rejects its admission as an aggravating circumstance and alleges these reasons:

"The Agency considers that, in accordance with the provisions of Recital 75 of the

GDPR, the passport number would be "particularly sensitive data insofar as

how much a third party can impersonate the identity of a natural person with total

ease, with the risks that this entails for privacy, honor and the

patrimony of the supplanted". "In our opinion, there are several considerations to take

consider. In these cases, the usurpation of identity occurs on a personal basis.

prior to contracting the prepaid line, that is: contracting the line

prepaid is a consequence of identity theft, not the usurpation of

identity in itself considered. That is to say, it is not that Vodafone with its conduct

provided personal data to a third party, 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 Vodafone itself.

On a purely theoretical level, the Agency's reasoning could reach

be admitted if the sanctioned party is responsible for conserving and preserving the security

the personal data of the data subject and, due to deficient security measures,

would allow a third party to gain illegitimate access to said data and, with this,

could impersonate the identity of the affected party. It is not the case."

VODAFONE invokes the circumstance of section b) of article 83.2 as mitigation.

of the GDPR: the absence of intent or negligence.

Finally, it proposes as evidence the admission of the following documents whose

copy provides:



1. Order sent to Vodafone by the Group for the Interception of

Telecommunications of the Civil Guard dated 03/10/2020 (document 1)

2. Vodafone's response to the order sent by the Interception Group

of Telecommunications of the Civil Guard (document 2)

3.Screenshot proving that the wholesaler who has signed a contract with

Vodafone is CSQ Non Stop Shop, S.L. who, in turn, contracted with the point of sale

responsible for registering the prepaid card in question, D.D.D. (document 3)

It also provides document number 4, "Non-exclusive Prepaid Wholesale Distribution

Vodafone".

The essential content of the documents provided is as follows:

1. Document 1 consists of two pages. Both carry in their head the

letterheads of the Ministry of the Interior and the Civil Guard. The first is the cover of

a fax sent by the Communications Interception Group of the Civil Guard to

VODAFONE on 03/10/2020 with this text: "Attached is a copy of the order

legal agreement: [...] Dilig. Previous: Police Diligences No. XX/XXXX. Affair:

Data. Telephone No.: ***PHONE.1 [...]"

The second is a copy of an Official Letter with the reference number "Police proceedings

***REFERENCE.3", the date 03/06/2020 and the subject "Requesting identification of the

owner of a telephone line. The addressee shows "Vodafone Company". He

The text of the Official Letter says that "because it is necessary for the investigations that are carried out

within the framework of the police proceedings ***REFERENCE.3 It is requested that they be

transferred to this Unit the following data: Ownership of the subscriber number

***PHONE.2 as of February 12, 2020."

2. Document 2 is VODAFONE's response to the Official Letter described in point

former. In the upper part it bears these indications: Judicial Police, Proceedings

Previous XX/XXXX; date of receipt 03/10/2020; response date 03/13/2020;

query type "LC.01.Holder by MSISDN and by date range"; Target

***PHONE.2 and search period from 2020-02-12 to 2020-03-02.

In the lower part it bears this information: Under the headings of "Name" and "Surname", the

name and both surnames of the claimant; under the heading “Document”

***REFERENCE.2; under the heading “Document Type”, “AR-Passport”; under the rubric

“Line” ***PHONE.2; under the heading “Type of contract”, “PREP”; under the rubric

“Registration Date”, 11/28/2019. The "Release Date" section is empty.

3. It is a screenshot in which there is no header or any data that allows

know its origin. It offers this information: On the first line appears "Date

request:” “11/28/2019”; “Locator IP”, an unreadable piece of information followed by “(...)”;

"Processor user: op_bot"; “Article: welcome Sim Yu YUSER 10”; “MSISDN

***PHONE.2”; "CSQ Center" and "D.D.D. Point of Sale."

4. The “Vodafone Non-exclusive Prepaid Wholesale Distribution” contract, entered into

between the defendant and CSQ Non Stop Shop, S.L., (CSQ) whose stipulation 12.2 says:

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

protection of personal data to retail outlets and will certify



have given notice of these obligations by signing a standard certificate

which is attached as Annex IV”. (The underlining is ours)

Attached to the contract is Annex II, “Data collection. Distribution contract

Wholesaler". It indicates that it "contains instructions relating to compliance with the

Sole Additional Provision of Law 25/2007 regarding (i) the identification

presence and collection of data from 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

in clause 11.2 of the Wholesale Distribution Contract from which this Annex brings

cause".

The first stipulation of the aforementioned annex establishes: "The Wholesaler must

transferred to the retail Point of Sale, by signing an agreement that

includes the obligations listed in this annex, the essential obligation

to identify the Client/Buyer PRESENTIALLY through his card

original identification. The documentation to be presented by natural persons, according to their

nationality and situation, is as follows: “-For Spanish nationals, DNI or NIF. -

For citizens of the European Community, DNI, Residence Card or

Passport.-For citizens from outside the European Community, Passport or NIE.”

(The underlining is ours)

The second stipulation of the Annex, "Data to be collected from purchasers of services

prepaid", it says in its section 1: "Individual person": "The Wholesaler must transfer to the

Retail Point of Sale the obligation to collect the following data of a nature

mandatory: Name, Surname, Nationality; Document type and number (DNI, NIF,

Passport, Residence Card).

The third stipulation of the Annex, "Printing and signature at the client's request", says: "In

if the customer requests it and the retail Point of Sale has enabled

Vodafone WAS or Web Service, from these tools a single

copy of the documentation (self-filled with the data entered in the

tools) and will be delivered to the Client/Buyer without the Point of Sale

Retailer can keep a copy of it.”

SIXTH: Practiced tests.

On 06/29/2022, the procedure instructor agrees to open a phase

of evidence and the practice of the following evidentiary procedures:

1. Consider reproduced for the purposes of evidence the claim filed by the

claimant and its attached documentation, as well as the documents obtained and

generated by the Data Inspection Sub-directorate of the AEPD during the phase of

admission to process the claim.

2. To consider reproduced for the purpose of proof the allegations to the initiation agreement

presented by VODAFONE and the accompanying documentation.

3. VODAFONE is requested to provide the AEPD with the following documentation and

information:

3.1. The copy of the Record of Treatment Activities (RAT) that had been approved

in November 2019.



3.2. The copy of the general conditions by which the company was governed in November 2019

relationship between the defendant and the customers who contracted a prepaid service with her.

3.3. To report whether the obligation to provide the general conditions to the client who

contracts a prepaid service corresponds to the retail point of sale. In case

In the affirmative, it is requested that you explain in which document this obligation of the

point of sale that intervened in the prepaid service that has originated this file

sanctioning. If not, explain and provide documentary evidence of when and

who was obliged to provide the customer who contracts a prepaid service with those

general conditions.

3.4. Annexes I, III, IV and V to the "Prepaid Wholesale Distribution Agreement. No

exclusive to Vodafone" that he celebrated with CSQ in June 2019.

3.5. The treatment order agreement that you signed with CSQ.

3.6. The contract that CSQ entered into with the retail outlet that intervened in the

contracting the prepaid service that is the subject of this sanctioning file.

3.7. The treatment commission agreement that CSQ would have signed with the point of

retail distribution that intervened in the contracting of the prepaid line, D.D.D.

3.8. That it inform how VODAFONE can prove that, indeed, the

point of sale collected from the person who requested the contracting of a prepaid line

your original identity document (not a photocopy), that verified your identity and that

collected the client's identity data from the aforementioned document.

SEVENTH: Response to the tests performed.

VODAFONE responds on 07/21/2022.

1. Provide (document 1) the RAT in force in the indicated period. He says that "This is the

registration of processing activities that applies to both franchises and

wholesalers." The document has the following characteristics: It has a heading

"Details of the processing activity" (Processing Activity Details). Information

It deals exclusively with "Distribution - Franchise Distributors". In it

section "Description of the treatment", mentions the "management of the

franchise" and says that the treatment is the same as in the stores owned by

VODAFONE 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 that is carried out, with respect to the

person in charge of treatment and the purposes of the treatment. It does not determine what

data is processed. Regarding the legal basis of the treatment, it says that "the

people have given their consent for the processing of their personal data

for one or several purposes."

2. It provides the general conditions of the prepaid mobile contracts used by

VODAFONE in 2019 (document 2) that are integrated by the "Rules of use

reasonable to the Vodafone Electronic Communications Services" and the

"Summary of General Service Conditions". Explain that these documents are

included in the packaging of the prepaid card and that the second document refers to the

operator's website to access the document provided with number 3.

3.As document 3, the "General Conditions of the Services of

Prepaid Mobile Communications" to which the customer accesses through the page



VODAFONE website. In its section 11, "Protection of Personal Data.",

establishes:

"According to the provisions of Organic Law 15/1999 on Data Protection of

personal character (LOPD), we inform you 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 with the

purpose of providing 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 with

after the validity of the contract. The aforementioned commercial actions are

may be made by any means of communication (telephone, e-mail,

sms, mms…); and (ii) install and update on your phone those applications

corresponding to telecommunications and value-added services

provided by Vodafone, by Vodafone Group companies or by third parties that

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 personal data

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

value-added services that involve said location and provided that

are previously requested by the Client and only for the time necessary to

lend them the same; d) transfer your personal data to Group companies

Vodafone (www.vodafone.es), all for the purpose of carrying out actions

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

paragraph of this Condition."

4. Provide Annexes I, III, IV and V to the Prepaid Wholesale Distribution Contract. No

Vodafone exclusive. Annex III corresponds to the order of treatment between

VODAFONE and CSQ. (Document 5)

5. Provide a copy of the contract that CSQ entered into with the retail Point of Sale that

intervened in the contracting of the prepaid service that is the subject of this file

disciplinary, D.D.D., and the order of treatment subscribed between both. (Document

6)

The contract, entered into on 04/20/2016 between CSQ and the Retail Point of Sale D.D.D.,

consists of some (i) "General Conditions applicable to the contract" and (ii) "of the

Specific conditions for the distribution of physical products that require the

Identification of the End User as a previous step for the sale, activation and/or

subscription of products or services.

Stipulation 1 of conditional (i) says that "The purpose of this contract is the

installation and operation of the Terminal owned by CSQ for recharging telephones

national and international mobiles on behalf of CSQ; leaving the possibility of

market other services and products through the Terminal whose conditions

They would be notified prior communication."



Conditional (ii) establishes:

1. "Object: In compliance with current legislation on

personal data protection,

the

determination by CSQ of the security measures that the Point of

Retail sale as "Treatment Manager", must adopt in the access

and processing of personal data for which CSQ is responsible for

treatment."

is the subject of this Contract

undertakes to

3.- "Security Measures." "The Point of

Sale

retail

implement the necessary technical and organizational security measures to:

• Guarantee confidentiality, integrity, availability and resilience

of treatment systems and services.

• Restore availability and access to personal data quickly,

in the event of a physical or technical incident.

• Verify, evaluate and value, on a regular basis, the effectiveness of the measures

technical and organizational procedures implemented to guarantee the safety of the

treatment.

With regard to identification and registration, the point of sale may not sell

no SIM without having completed the following procedure:

a) The Retail Point of Sale accepts the use of the tools that for

for this purpose CSQ has, and in some cases it will imply the use of the own

tools specified by the different telephone operators (eg:

Vodafone WAS), committing to incorporate only the data of

buyer requested in the corresponding activation section

b) Prior to the sale, the Point of Sale will identify the Final Customer

through face-to-face validation of a document proving your identity,

It must be valid, original and in force. Specific:

• The mandatory data for natural persons are: Name, Surname,

Nationality, Type and number of document (DNI, NIF, Passport, Card of

Home).

• The mandatory data for legal persons are: Company name, Type and

tax identification number and full address

• In both cases, it is mandatory to identify the Buyer in person

through the original documentation requested in each case, and verify that

the data provided and recorded in the CSQ activation system are

correct, truthful and up-to-date and correspond to the

documentation provided.

c)

[...]

Prior to the identification and registration of the data, the Point of Sale

will inform the End Client about the legal obligation to identify themselves in the

terms of the previous paragraph and provide all the information indicated therein,

indicating that the supply of the same is mandatory for activation and

provision of the service.

CSQ is not responsible for the veracity of the data provided, being

sole responsibility of the point of sale to have verified the information with

a valid supporting document. The point of sale declares by signing

this document to be aware that, in the event that you misuse the

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

16/51

activation tool provided by CSQ or by any third party

telephone operator (eg Vodafone WAS), or enter wrong data in the

same from buyers of prepaid services, you may be limited or withdrawn

access to the activation tool, also leaving CSQ and/or the

operator, as appropriate, empowered to claim at the point of sale, for

any way, the damages and losses actually caused as

consequence of such misuse. (The underlining is ours)

6. To the question regarding how he could prove that, indeed, the point of sale

obtained from the person who requested the contracting of a prepaid line his document

Original identity card (not a photocopy), which verified your identity and which you obtained from the aforementioned

document the identity data of the client, responds in these terms:

"As indicated in the pleadings to the Commencement Agreement, CSQ 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

physical persons consists of the "DNI or NIF" or the "Passport or NIE"

(Document 4 of the brief of Allegations to the Commencement Agreement).

In turn, this obligation was transferred to the point of sale (D.D.D.), as

certifies Document 6 provided with this document:

"b) Prior to the sale, the Point of Sale will identify the Final Customer

by validation

in person of a document proving your identity, which must be valid

original and current. Specific:

• The mandatory data for natural persons are: Name, Surname,

Nationality, Type and number of document (DNI, NIF, Passport, Card of

Home).

• The mandatory data for legal persons are: Company name, Type and

tax identification document number and full address.

• In both cases, it is mandatory to identify the Buyer in person

by means of the

original documentation requested in each case, and verify that the data

provided and those recorded in the CSQ activation system are

correct, truthful and up-to-date and correspond to the

documentation provided."

EIGHTH: Resolution proposal.

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

following terms:

<<That the Director of the Spanish Data Protection Agency 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, with a fine of €100,000

(one hundred thousand euros).>>

The certificate issued by the FNMT that is in the file certifies that the

Notification was accepted by the defendant on 10/17/2022.



Pursuant to article 73.1 of the LPACAP, the term to make allegations is ten

business days that must be computed from the day following the acceptance of the

notification. Thus, having accepted the notification of the proposed resolution

On 10/31/2022, the claim period ends on 10/31/2022.

NINTH: Request for extension of the term of allegations to the proposal of

resolution.

On 10/18/2022, the AEPD received a letter from VODAFONE in which

requests that the period granted for

make 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 and is accepted on 10/24/2022 according to

it appears in the certificate issued by the FNMT that is in the file.

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

they were practiced before VODAFONE itself.

It was added that the defendant had had the opportunity to provide evidence in the

procedures of allegations to the initiation agreement and in the test phase and that the proposal

resolution maintained the legal qualification of the facts that made the agreement of

beginning, limiting itself, in essence, to rebutting the arguments that the defendant had

used in his defense in the allegations to the opening agreement.

TENTH: VODAFONE does not formulate allegations to 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

in the file, the following have been accredited:

PROVEN FACTS

FIRST: The claimant denounces that VODAFONE registered a prepaid line

linked to your personal data; data that he provided to the Civil Guard and for which he has

summoned by two courts as being investigated as a consequence of the

scams committed through Wallapop by the telephone line that VODAFONE

linked to his person.

SECOND: There are two screenshots in the file from your

systems, obtained on 05/06/2021, which VODAFONE sent to the Sub-directorate of

Data Inspection with its response to the information request. Both

correspond to "Customer Interaction Manager" and they display these

windows:

(i) "Caller Information", which includes, among others, the "ID" tabs,

“***REFERENCE.4”; and “Client”, “A.A.A..”

(ii) "Central Information Page", with several tabs, two of which,

“Contact Information” and “Contracted Services,” are turned on and their results

are shown in respectively, in the two screenshots provided by the

claimed:

-

-

contact"

The window "Information of the

space

“NIF/NIE/Passport/Cif:” “***REFERENCIA.2” and in “Status” “Disconnected”.

The "Contracted Services" window includes in the description of the services

basic, the "prepaid telephone price plan". As equipment indicates

***TELEPHONE 1; as “Device type”, “Mobile Pre.”; such as “Status”, “Desc.”

as F. Installation”, “28/11/2019” and as “F. Desins”, “07/19/2020”.

includes in the

THIRD: The copy of the fax that the Group for the Interception of

Civil Guard Communications sent on 03/10/2020 to VODAFONE with this

text:

“Attached is a copy of the court order agreeing: [...] Dilig. Previous:

Police proceedings No. XX/XXXX. Subject: Data. Telephone No.: ***PHONE.1

[...]”

Work in the file the copy of the Official Letter sent to the defendant - number of

reference "Police proceedings ***REFERENCE.3" and dated 03/06/2020- with the

subject "Requesting identification of the owner of a telephone line". The text of the Office

is the following:

“[...]because it is necessary for the investigations carried out within the framework of

the police proceedings ***REFERENCE.3 It is requested that they be transferred to this

Unit the following data: Ownership of the subscriber number

***PHONE.2 as of February 12, 2020.”

FOURTH: VODAFONE's response to the cited Official Letter is in the file: A

screenshot including this information:

At the top of the document”: “Judicial Police, Preliminary Proceedings XX/XXXX”; the

date of receipt, 03/10/2020; the response date, 03/13/2020; the type of query,

"LC.01. Holder by MSISDN and by range of dates"; the “Target”, “***PHONE.2” and the

search period: from 2020-02-12 to 2020-03-02.

At the bottom, the name and both surnames of the claimant; as "Document",

“***REFERENCE.2”; as "Document Type", "AR-Passport"; as "Line",

***PHONE.2; as "Type of contract", "PREP"; as "Add Date", 11/28/2019. He

"Release Date" section is empty.

FIFTH: There are several documents in the file from the Civil Guard, Post of

*** LOCATION.2, which show that the Civil Guard identified the claimant as

holder of the mobile line *** TELEFONO.1 by virtue of the answer that VODAFONE

made it easy for him Among these documents is the "Diligence consigning identification of

a person":

"In ***LOCATION.2, being (...) March 24, 2020, by this Diligence

it is stated that, as a consequence of the steps taken, there have been

obtained the identification data of the person indicated below

whose data are: Name: A.A.A. (DNI ***NIF.1)". The document includes the date

of birth of the claimant, the name of her mother and father and a

address and adds: "It is hereby stated that the identification was made

by answering VODAFONE as the holder of the telephone number

***TELEPHONE.1, cited by the complainant[...]

"In ***LOCATION.2, being (...) March 24, 2020, by this Diligence

it is stated that, as a consequence of the steps taken, there have been

obtained the identification data of the person indicated below

whose data are: Name: [name and two surnames of the claimant] (DNI

***NIF.1).

[...]

Date of Birth: 04-24-198j

Father's name: B.B.B.

Mother name: C.C.C.

Address: ***ADDRESS.1.

It is stated that the identification was made by answering

VODAFONE as the owner of the phone number ***TELEFONO.1, quoted by the

complainant.

The person identified in this proceeding is aware of another address in

DGT Database, being the following: ***ADDRESS.2 [...]”

SIXTH: VODAFONE denies that article 6.1 of the GDPR has been violated and

considers that the legality of the treatment was founded on the legal bases of the

article 6.1.b) and 6.1.c)

SEVENTH: VODAFONE states that "security measures were implemented

necessary and the third party that committed the fraud exceeded the Security Policy to

Private Clients, providing the information of the interested party that would have been obtained

by illegal or fraudulent means. Named Security Policy for Clients

Individuals to the "Prepaid Wholesale Distribution" contract. Not exclusive Vodafone”

(document 4, annex to its allegations to the initiation agreement) signed between the

claimed and CSQ Non Stop Shop, S.L. (CSQ)

EIGHTH: Stipulation 12.2 of the contract for "Prepaid Wholesale Distribution Not

exclusive Vodafone”, held between the defendant and CSQ 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 Annex IV". (The underlining is ours)

Annex II to the Wholesale Distribution contract - "Data collection. Contract of

Wholesale Distribution"- says in its first stipulation:

"The Wholesaler must transfer to the retail Point of Sale, through the

subscription of an agreement that includes the obligations related in the

present annex, the essential obligation to identify PRESENTIALLY

to the Client/Buyer by means of their original identification card.

The

Documentation to be presented by natural persons, according to their nationality and

situation is as follows: "-For Spanish nationals, DNI or NIF. -For

Citizens of the European Community accept DNI, residence card or

Passport. -For citizens from outside the European Community, Passport or

NIE." (The underlining is ours)

The second stipulation of the Annex says:

"Data to be collected from buyers of prepaid services," it says in its

Section 1: "Individual person": "The Wholesaler must transfer to the Point of Sale

retailer the obligation to collect the following mandatory data:

Name, Surname, Nationality; Document type and number (DNI, NIF,

Passport, Residence Card).

NINTH: The contract that CSQ entered into with the Point of Sale is in the file

retailer that intervened in the contracting of the prepaid service object of this

disciplinary file, D.D.D., and the treatment order signed between them.

(Document 6)

The "Specific conditions for the distribution of

physical products that require the identification of the End User as a previous step

for the sale, activation and/or subscription of products or services.", of which

transcribe these stipulations:

“3.- “Security Measures.” "The Retail Point of Sale is committed to

implement the necessary technical and organizational security measures to:

[...]

With regard to identification and registration, the point of sale may not sell

no SIM without having completed the following procedure:

to)

b) Prior to the sale, the Point of Sale will identify the Final Customer

through face-to-face validation of a document proving your identity,

It must be valid, original and in force. Specific:

• The mandatory data for natural persons are: Name, Surname,

Nationality, Type and number of document (DNI, NIF, Passport, Card of

Home).

• Mandatory data for legal entities [...]

• In both cases, it is mandatory to identify the Buyer in person

through the original documentation requested in each case, and verify that

the data provided and recorded in the CSQ activation system are



correct, truthful and up-to-date and correspond to the

documentation provided.

c)

[...]

Prior to the identification and registration of the data, the Point of Sale

will inform the End Client about the legal obligation to identify themselves in the

terms of the previous paragraph and provide all the information indicated therein,

indicating that the supply of the same is mandatory for activation and

provision of the service."

TENTH: To the question regarding how he could prove that, indeed, the point

of sale obtained from the person who requested the contracting of a prepaid line his

original identity document (not a photocopy); who verified his identity and who collected

of the aforementioned document the customer's identity data, VODAFONE responds in

these terms:

"As indicated in the pleadings to the Commencement Agreement, CSQ 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

physical persons consists of the "DNI or NIF" or the "Passport or NIE"

(Document 4 of the brief of Allegations to the Commencement Agreement).

In turn, this obligation was transferred to the point of sale (D.D.D.), as

certifies Document 6 provided with this writing:

"b) Prior to the sale, the Point of Sale will identify the Final Customer

through face-to-face validation of a document proving your identity,

It must be valid, original and in force. Specific:

• The mandatory data for natural persons are: Name, Surname,

Nationality, Type and number of document (DNI, NIF, Passport, Card of

Home).

• [..].

• In both cases, it is mandatory to identify the Buyer in person

through the original documentation requested in each case, and verify that

the data provided and recorded in the CSQ activation system are

correct, truthful and up-to-date and correspond to the

documentation provided."

ELEVENTH: In response to the request to provide evidence a copy of the

RAT in force in November 2019, VODAFONE provides a document (number 1)

on which it says: "This is the record of processing activities that is applied

both franchises and wholesalers."

The information in the document provided deals exclusively with "Distribution -

Franchise Distributors". In the "Description of treatment" section, mention the

"management of franchise stores" and says that the treatment is the same as in the

VODAFONE own stores with two differences. It does not determine what data is

treatment object. Regarding the legal basis of the treatment, it indicates that "the

people have given their consent for the processing of their personal data

for one or several purposes."



FUNDAMENTALS OF LAW

Yo

Competition of the AEPD

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

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

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

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

digital rights (hereinafter, LOPDGDD), is competent to initiate and resolve

this procedure the Director of the Spanish Data Protection Agency.

Likewise, article 63.2 of the LOPDGDD determines that "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

applicable provisions

The RGPD deals in its article 5 with the principles that govern the treatment of personal data.

personal data and establishes that "1. Personal data will be:

a) Treated in a lawful, loyal and transparent manner with the interested party (<<legality, loyalty and

transparency>>.

(...)"

Point 2 of article 5 indicates that "The person responsible for the treatment will be responsible

of compliance with the provisions of paragraph 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 personal 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."

Infringement of article 6.1 of the GDPR

II

The defendant in the start-up agreement was attributed a violation of article 6.1 of the

GDPR materialized in having processed the personal data of the claimant linked

to a prepaid line, number ***TELEPHONE.1, to which the claimant was unrelated, without

that none of the legal bases of legality that relates to that provision concur.

1. Data of the claimant who have been subject to treatment.

The documentation in the file proves that the claimant's data

illegally processed by VODAFONE were the name, the two surnames and his phone number

passport, ***REFERENCE.2.

In the second Proven Fact, the information contained in the two

screenshots of the VODAFONE systems that the entity provided to the

Sub-directorate of Data Inspection when responding to transfer actions

carried out in accordance with article 65.4 of the LOPDGDD. It is thus verified that, in their

systems, these data were registered: With the ID ***REFERENCE.4 there was a

client with the name and both surnames of the claimant and with the passport

***REFERENCE.2 as holder of a prepaid mobile service ***TELEPHONE.1,

being the dates of discharge and discharge from the service -different from the completion of the treatment

of the data- respectively, on 11/28/2019 and 07/19/2020.

Regarding the passport number processed by VODAFONE, there is no doubt that

that we are dealing with personal data of the claimant. The documentation that works in

the file reveals that it was through that personal data -the passport number-

as the Civil Guard identified the claimant by her DNI and was also able to know her

address and filiation information.

VODAFONE responded on 03/13/2020 to an Official Letter sent to it on 03/10/2020 by the Group

Interception of Communications of the Civil Guard with the matter "Requesting

identification of the owner of a telephone line. The defendant provided the name and

surname of the claimant, the passport number ***REFERENCE.2, the indication

that it was a prepaid mobile line and the registration date, 11/28/2019.

In the "Proceedings consigning identification of a person" issued by the post

of the Civil Guard of *** LOCATION.2 (Fifth Proven Fact) the Civil Guard

already knows the DNI data linked to the owner of the controversial line, his address and

your affiliation data. The Diligence says “[...] that, as a consequence of the efforts

practiced, the identification data of the person indicated below have been obtained.

below whose details are: Name: [name and two surnames of the claimant]

(DNI ***NIF.1).

[...]

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

24/51

Father's name: B.B.B.

Mother name: C.C.C.

Address: ***ADDRESS.1.”

The Diligence adds that "It is stated that the identification has been made

by answering VODAFONE as the holder of the telephone number

***TELEPHONE.1, summoned by the complainant.

The person identified in this proceeding is aware of another address in Base de

DGT data, being the following: ***ADDRESS.2 [...]” (The underlining is ours)

Among the identifying data of the claimant that the Civil Guard reflects in the

Identification procedure includes the DNI, the address and the name of the father and the

mother. Data that VODAFONE did not know and could not have provided to the Civil Guard

but that have been obtained by the remission that the passport number makes to the number

of the DNI.

We must refer to Royal Decree 896/2003, of July 11, which regulates the

"issuance of the ordinary passport and determines its characteristics and content". He

Article 10, "Content" says in section 2 that the passport "will have a

laminated page that will contain the following mentions:

a) The passport number, which will coincide with the serial of the book.

b) A personal identification number that will be that of the national identification document.

identity of its owner, unless it lacks it, for being a resident in the

foreigner or under 14 years of age, [...]

c) The issuing office number.

d) Surnames, first name, nationality, date and place of birth and sex, as well as

such as the issuance and expiration dates of the passport. will contain,

likewise, the digitized signature of the owner, for which purpose, to provide it, you must

Go to the issuing units. [...]

e) The digitized photograph of the holder.

f) Two lines of OCR characters [...]" (The underlining is ours)

Article 10 of Royal Decree 896/2003, says in section 5:

"5. The passport will incorporate an electronic chip that will contain the

following information referring to its owner: affiliation data, digitized image

of the photograph, fingerprints of the index fingers of both hands, or

those that, in their absence, correspond according to the following order of priority:

middle, ring or thumb."

Consequently, the regulations governing the passport determine its content and

Pursuant to this provision, it includes, on the laminated page, the number of

Owner's ID. It is evident that, when a natural person is identified by the number of

passport – which, in this case, is the personal data of the claimant that VODAFONE

collected from the purchaser of the prepaid line and kept in their files for more than

a year - it has been possible to know your ID and the data that are part of the content of

this document, such as address; data that, on the contrary, is not included in the

passport, not even in the embedded electronic chip, referred to in point 5

of article 10 of Royal Decree 896/2003.

2. Fundamentals of the legality of the treatment invoked by VODAFONE.

The defendant has denied in her allegations that the treatment she made of the data personal information of the claimant -passport number, name and surname- violates the article 6.1 of the GDPR. It maintains that this treatment was covered by two of the bases of legality of the precept indicated:

(i) paragraph c), the processing is necessary for the fulfillment of an obligation imposed on the person responsible for the treatment by the Law of the Union or of the Member States and

(ii) section b), the treatment is necessary for the execution of the contract.

2.1

. Legitimation based on section c) of article 6.1. GDPR.

2.1.1. VODAFONE maintains in defense that its conduct was adjusted to Law that the processing of the personal data of the claimant who is the object of the claim was based on section c) of article 6.1 of the GDPR in connection with the legal obligation imposed by the Sole Additional Provision of Law 25/2007, of October 18, of conservation of data related to communications electronic networks and public communications networks (hereinafter Law 25/2007) which states:

“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 warns that "identifying data" will be

subject to the provisions of Law 25/2007. Among those provisions of the Law

25/2007 it is worth mentioning article 8, "Protection and security of data", which

establishes:

"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)

References to Organic Law 15/1999 on the Protection of Personal Data

Personal (LOPD) must be understood as currently made to the RGPD and the LOPDGDD.

Therefore, the processing of personal data that the operators carry out under the

of Law 25/2007 is subject, in any case, to the data protection regulations of

personal character. This is also confirmed by the Council of State in its Opinion

32/2007, of February 22, 2007, issued in relation to the Draft Law on

conservation of data related to electronic communications and networks

public communications in which, with regard to the data processed in

application of the Sole Additional Provision, mentions, reiterating it, the criterion of

Legal Office of the AEPD in its 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)."

2.1.2. Sole Additional Provision of Law 25/2007.

It is necessary to examine next what is the content and the raison d'être of the

obligation that the Unique Additional Provision of Law 25/2007 imposes on

telephone operators, in this case to 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, in which the defendant intends to

justify the legality of the treatment object of the claim and that, in its allegations

to the initiation agreement, it has referred to the Sole Additional Provision as "the rod of measure that must be taken by Vodafone and the rest of the operators."

The purpose pursued with the obligation contained in this provision is to contribute to the fight against crime, providing the authorities with the competence of ensure the public safety of an instrument that allows them to control the use of those devices for criminal purposes. The Preamble of 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.

Regarding the content of the imposed obligation, it should be noted that it is not reduced to the fact that 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 of 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 acknowledge that he has to make that

the person of the acquirer "is the same as the one assumed [..]", is carried out through



a "document accrediting personality". In our legal system, if

well that document is, par excellence, the "national identity document" or "DNI",

the only one that by itself proves the identity of its owner, the

passport among the means that identify the physical person.

Organic Law 4/2015, of March 30, on the protection of citizen security (in

onwards Organic Law 4/2015) dedicates Chapter II to "Documentation and

personal identification". In accordance with the provisions of Chapter II, the

Documents that fulfill the purpose of identifying people are:

(i) the DNI, regulated in articles 8 to 10 defined in article 8.1. as a

public and official document and will have the protection granted to them by law. Is he

only document with sufficient value on its own for accreditation, to all

effects, of the identity and personal data of its owner."

(ii) the passport, regulated in article 11.

(iii) proof of identity of foreign citizens, article 13.

Article 11, "Passport of Spanish citizens", provides that "1. The passport

Spanish is a public, personal, individual and non-transferable document that, except

proof to the contrary, certifies the identity and nationality of Spanish citizens

Outside of Spain, and within the national territory, the same circumstances of the

non-resident Spaniards. (The underlining is ours)

The reference that the Additional provision of Law 25/2007 makes to the means of

identification, to the "document" accrediting personality, implies that the operator

You have to physically access the document. The use of the

photocopy, since it lacks the security guarantees that the document enjoys

original. Regarding the passport, we refer to Royal Decree 896/2003

which in its article 10 regulates the content of the passport and establishes in section 5:

"5. The passport will incorporate an electronic chip that will contain the

following information referring to its owner: affiliation data, digitized image

of the photograph, fingerprints of the index fingers of both hands, or

those that, in their absence, correspond according to the following order of priority:

middle, ring or thumb."

2.1.3. Treatments whose legality can be protected in article 6.1.c) of the GDPR in

connection with the Single Additional Provision.

Based on 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 fundamental

validity of the legality of the treatment that the telephone operators make of the data

personal information of which smart card purchasers are holders. Always

that the data processing carried out by the operator is limited and has only

as a purpose to comply with the provisions of Law 25/2007.

It should be noted, in this sense, 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 purposes other than that pursued by the Sole Additional Provision, of the

data collected in compliance with that provision, such as



connected with the development and execution of the contract. The treatments that

eventually carried out by the operator for another purpose must be based on some

of the legal bases described in article 6.1. of the GDPR other than the one that has been

mentioned.

Regarding the case at hand, we must conclude that it is not possible to accept the

the thesis of the defendant and protect the legality of the treatment that VODAFONE made of the

personal data of the claimant, the number of her passport and her name and

surnames, on the legal basis of section c) of article 6.1 of the GDPR in relation to

the Unique Additional Provision of Law 25/2007.

The obligation that Law 25/2007 imposes on telephone operators, connected with

Article 6.1.c) of the GDPR, empowers operators, exclusively, to process the

data of the holders of the persons who acquire a prepaid card; of

so that the processing of data that does not identify the purchaser of that type of services is outside the coverage of the aforementioned Additional provision. One has to therefore reject VODAFONE's assertion that it is bound by the Law 25/2007 to treat the "name and surname of the buyer", as well as the "number corresponding to the identification document used" by the buyer of the card prepaid". (The underlining is from VODAFONE)

As 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 to the purchaser of a prepaid card -especially if the data is the passport number, since it unequivocally identifies the Spanish citizens unless proven otherwise - prevents this treatment from being considered lawful on the basis of article 6.1.c) of the GDPR in connection with the provision of the Law 25/2007. Provision that, as has been said, imposes on the operator the obligation to collect the data that identifies the acquirer of the smart card but not the third party data.

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 "name and surname of the buyer", as well as the "number corresponding to the identification document used" by the purchaser of the prepaid card; a different matter is that such

data turn out to be erroneous, but this may not imply, in any case, a

infringement of article 6.1 of the GDPR." (The underlining is from VODAFONE)

On the other hand, VODAFONE has recognized in its allegations to the start-up agreement

(Third allegation) that the passport information of the claimant who was subject to



treatment linked to the prepaid line did not belong to the purchaser of the card. The

entity said:

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

personal information 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."

Thus, the conduct of VODAFONE that is the subject of analysis in this

sanctioning file constitutes an illegal treatment of the personal data of the

claimant -his passport number and his name and surname- and violates article 6.1

of the GDPR. The defendant processed the data of the claimant's passport number and did not

that of the purchaser of the prepaid service, the only piece of information that was authorized to collect

tenor of the legal obligation whose compliance has been invoked: the Additional provision

Unique of Law 25/2007.

2.1.4. On the alleged absence of guilt.

Being accredited the existence of an unlawful conduct of VODAFONE -the

treatment of the claimant's data without a legal basis- the question centers on

determine whether such conduct may give rise to administrative responsibility

sanctioning.

The defendant has requested in her allegations, on a subsidiary basis, that this

Agency agrees to file the procedure for non-existence of guilt.

VODAFONE dedicated the second allegation of its pleadings to the agreement of

I begin to defend that, regarding the unlawful conduct that has been accredited,

no guilt of any kind intervened on his part and to request, consequently, that

proceed to file the file due to the non-existence of the necessary element of the

culpability.

He invoked different arguments to justify the absence of guilt in his conduct:

a fraud that "has generated that in the systems of my represented

registered a prepaid line in the claimant's name using a passport

invalid. In this case, security measures were implemented from Vodafone

necessary and the third party that committed the fraud exceeded the Security Policy to

Private Clients, providing the information of the interested party that would have been obtained

by illegal or fraudulent means. A criminal practice in which a third party overcame

established controls (we are “facing a criminal practice carried out by a

third party who, acting fraudulently, has supplanted the identity of the Claimant to the

request the registration of a prepaid card on behalf of the Claimant, exceeding the

controls established by Vodafone.”). Or the existence of a human error that, he says,

is unavoidable and cannot be controlled (“[...], the fact of processing personal data that

belonged to the Claimant has been due to the existence of a human error, which

they are unavoidable and over which Vodafone cannot have effective control. [...],

there may be cases, such as this one, in which Vodafone processes personal data

that do 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.”)

Strict liability is proscribed in our legal system. In it
scope of sanctioning Administrative Law governs the principle of guilt,
way that the subjective or guilty element is an indispensable condition for
that the sanctioning responsibility arises. Article 28 of Law 40/2015, of
Legal Regime of the Public Sector (LRJSP) regulates the principle of guilt and
has:

"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.

The Constitutional Court, among others, in its STC 76/1999, has declared that the
Administrative sanctions participate of the same nature as criminal ones, being
one of the manifestations of the ius puniendi of the State, and that, as a requirement
derived from the principles of legal certainty and criminal legality enshrined in the
articles 9.3 and 25.1 of the CE, its existence is essential to impose them.

With regard to the guilt of the legal person, it is worth mentioning STC 246/1991, 19
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)

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 demanded. This is how he recognizes it

the same operator claimed when echoing the pronouncement of the STS of

01/23/1998 in which, as stated, the Court declared that "for the exculpation

the invocation of the absence of guilt will not 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 is doing by arguing that by not having prevented the security measures
security the result there is guilt. Far from it what must be done and is missed
least in the Resolution is to analyze the sufficiency of the measures from the
average diligence parameters required in the data traffic market. Well if I know
works with full diligence, scrupulously fulfilling the duties derived from
acting diligently, it is not possible to affirm or presume the existence of any fault." (He
underlined is from 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)

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 controller 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.

Opinion 3/2010, of the Article 29 Working Group (GT29) -WP 173- issued

during the validity of the repealed Directive 95/46/CEE, but whose reflections are

currently applicable, states that the "essence" of proactive responsibility is

the obligation of the data controller to apply measures that, in

normal circumstances, ensure that in the context of security operations

treatment, the regulations on data protection are complied with and in having

available documents that demonstrate to the interested parties and to the Authorities of

control what measures have been adopted to achieve compliance with the standards in

data protection matter.

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 processing

as well as risks of varying probability and severity for the rights and

freedoms of natural persons, the data controller will apply measures



appropriate technical and organizational in order to ensure and be able to demonstrate that the

treatment is in accordance with this Regulation. These measures will be reviewed and

They will update when necessary.

2. When they are provided in relation to the treatment activities, among

The measures mentioned in section 1 will include the application, by the

responsible for the treatment, of the appropriate data protection policies.

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

responsible for the treatment." (The underlining is ours)

Article 25 of the GDPR, "Data protection by design and by default", provides:

"1.Taking into account the state of the art, the cost of the application and the nature,

scope, context and purposes of the processing, as well as the risks of varying probability and

seriousness of the treatment for the rights and freedoms of individuals

physical, the data controller will apply, both at the time of determining the

means of treatment as at the time of the treatment itself, technical measures and

appropriate organizational measures, such as pseudonymization, designed to effectively apply

effective data protection principles, such as data minimization, and

Integrate the necessary guarantees in the treatment, in order to meet the requirements of the

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 was precise to fulfill the obligations that

imposes the Unique Additional Provision of Law 25/2007, in relation to 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 October 17, 2007 (Rec. 63/2006), which, after

refer to the fact that the entities in which the development of their activity entails a

continuous treatment of customer data and third parties must observe an adequate

level of diligence, says: "[...] the Supreme Court has understood that there is

recklessness whenever a legal duty of care is neglected, that is, when the

offender does not behave with the required diligence. And in the assessment of the degree of

diligence, the professionalism or not of the subject must be specially considered, and not

there is no doubt that, in the case now examined, when the activity of the appellant

is of constant and abundant handling of personal data, it must be insisted on

the rigor and exquisite care to comply with the legal provisions in this regard". (He

underlined is from the AEPD)

VODAFONE defends that, in compliance with the obligation imposed by the Law

25/2007, observed all the diligence that was required. To check the reality of

this statement nothing better than examining what were the measures actually

adopted by the defendant aimed at the proper identification of the purchaser of a

prepaid service.



VODAFONE was asked in the test phase how it could prove to the AEPD that

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

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

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

customer identity. The defendant responded in these terms:

"As indicated in the pleadings to the Commencement Agreement, CSQ 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

physical persons consists of the "DNI or NIF" or the "Passport or NIE"

(Document 4 of the brief of Allegations to the Commencement Agreement).

In turn, this obligation was transferred to the point of sale (D.D.D.), as

certifies Document 6 provided with this document:

"b) Prior to the sale, the Point of Sale will identify the Final Customer

through face-to-face validation of a document proving your identity,

It must be valid, original and in force. Specific:

• The mandatory data for natural persons are: Name, Surname,

Nationality, Type and number of document (DNI, NIF, Passport, Card of

Home).

• [..].

• In both cases, it is mandatory to identify the Buyer in person

through the original documentation requested in each case, and verify that

the data provided and recorded in the CSQ activation system are

correct, truthful and up-to-date and correspond to the

documentation provided." (The underlining is ours)

Effectively both contracts, the one for Wholesale Distribution and the one signed between that

distributor and the point of sale, included the obligation to identify in person the

client through an original document and, in addition, the first of them the obligation to

inform the point of sale of this obligation. On the other hand, the only forecast that

exists in the aforementioned contracts - Wholesale Distribution and the one signed between the wholesaler

and the Point of Sale - that could be interpreted as an attempt, even if formal, to

control compliance with the obligations assumed by the person in charge and sub

in charge, is that the Wholesale Distributor issues a document in which

certify that you have informed the points of sale of the obligation to identify the

purchasers of prepaid cards under the terms provided in the Provision

Additional to Law 25/2007 and in the Wholesale Distribution contract entered into with

VODAFONE. The certificate has not been provided by VODAFONE as proof of the

diligent action that says to observe.

Stipulation 12.2 of the "Non-exclusive Prepaid Wholesale Distribution" contract

Vodafone", held between the defendant and CSQ 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 Annex IV". (The underlining is ours)



Annex II to the Wholesale Distribution contract - "Data collection. Contract of

Wholesale Distribution"- says in its first stipulation:

"The Wholesaler must transfer to the retail Point of Sale, through the

subscription of an agreement that includes the obligations related in the

present annex, the essential obligation to identify PRESENTIALLY

to the Client/Buyer by means of their original identification card.

The

Documentation to be presented by natural persons, according to their nationality and

situation is the following:

“-For Spanish nationals, DNI or NIF.

-For citizens of the European Community, DNI, Card of

residence or Passport

-For citizens from outside the European Community, Passport or NIE.”

(The underlining is ours)

The second stipulation of the Annex says:

"Data to be collected from buyers of prepaid services", it says in section 1:

"Individual person": "The Wholesaler must transfer to the Retail Point of Sale the

obligation to collect the following mandatory data: Name, Surname,

Nationality; Type and number of Document (DNI, NIF, Passport, Card of

Home)."

Work in the file, provided by VODAFONE, the contract that CSQ entered into with the

Retail Point of Sale that intervened in the contracting of the prepaid service object

of this disciplinary file, D.D.D., and the processing order signed between

both (Document 6) Among the conditions that make up this document are the following:

“Specific conditions for the distribution of physical products that require the

Identification of the End User as a previous step for the sale, activation and/or

subscription of products or services. In its stipulation 3, "Security Measures",

it is established that:

"The Retail Point of Sale undertakes to implement security measures

technical and organizational security necessary to:

[...]

With regard to identification and registration, the point of sale may not sell

no SIM without having completed the following procedure:

to)

b) Prior to the sale, the Point of Sale will identify the Final Customer

through face-to-face validation of a document proving your identity,

It must be valid, original and in force. Specific:

• The mandatory data for natural persons are: Name, Surname,

Nationality, Type and number of document (DNI, NIF, Passport, Card of

Home).

• Mandatory data for legal entities [...]

• In both cases, it is mandatory to identify the Buyer in person

through the original documentation requested in each case, and verify that

the data provided and recorded in the CSQ activation system are

correct, truthful and up-to-date and correspond to the

documentation provided.

c)

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

36/51

[...]

Prior to the identification and registration of the data, the Point of Sale

will inform the End Client about the legal obligation to identify themselves in the

terms of the previous paragraph and provide all the information indicated therein,

indicating that the supply of the same is mandatory for activation and

provision of the service."

The lack of diligence shown by VODAFONE in its

obligation to keep a Record of Treatment Activities (RAT), a deficiency that

has a direct impact on the probability that timely action will be taken

to guarantee compliance with the principle of legality with respect to data such as the NIF whose treatment is not recorded.

Article 30 of the GDPR requires that it describe, among others, "the categories of personal data". In response to the request made to the defendant in the phase of proof for the RAT to provide, the document that you have provided versa exclusively on the activity of the Distributors -Franchise- and does not no reference to the NIF data or the identification documents that must be collected on the occasion of the sale of prepaid products. Nor does it mention any of the legal bases that you have invoked as the legal basis of the treatment (Articles 6.1.c of the GDPR in relation to the Additional provision of Law 25/2007 and 6.1.b) but rather contemplates as a legal basis that "people have given their consent to the processing of your personal data for one or more purposes".

VODAFONE's security policy that that entity alleges was surpassed by who acting fraudulently supplanted the identity of the claimant, is reduced, in the practice, to be included in the contracts signed with the wholesale distributor and between it and the point of sale the obligation to identify the purchaser of the prepaid service with according to the Additional provision of Law 25/2007.

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.

As a result, 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

Finally, what is alleged by VODAFONE regarding the

considerations that were made by the Agency in the agreement to initiate this

procedure: It was said in the initiation agreement that "the principle of responsibility

proactive (article 5.2 GDPR) obliges the controller to adopt the necessary measures

to be in a position to demonstrate that the treatment was founded on some

of the circumstances listed in article 6.1. GDPR; for what matters here,

that the person who contracted the controversial line and identified himself with the name and two



surname of the claimant and with the passport number ***REFERENCE.2, was

really owner of the data provided as their own.”

It was added that "so that the data processing carried out by the defendant could

be based on any of the legitimizing circumstances of the treatment would be

necessary that, in his capacity as data controller, he could prove that the

The owner of the processed data was effectively the one who provided them and signed the

contract to which they were bound."

It was also indicated that, "However, the defendant has not provided her response to

the request for information prior to the admission of this claim for processing, no

document or evidence that proves the legal basis of the

treatment carried out. Neither has he provided any document that demonstrates the

origin of the data processed - which were provided by the person who celebrated the

contracted- or that on the occasion of the contracting he requested and obtained from the contracting party the documentation proving that he was the owner of the data provided as his."

"In this sense, the defendant did not provide SETID, within the framework of the procedure filed before it by the claimant, the contract documentation linked to the controversial line, arguing then that there was no contract linked to the NIF of the claimant given that in contracting the The person who intervened did not identify himself with that information but with a passport number."

For all these reasons, in the opening agreement it was estimated 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 opening agreement, VODAFONE stated the following in its allegations:

"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, that measures be implemented, such as, for example, a ID and passport scanning and verification software.

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.

That said, if the Agency intends to modify those requirements and increase the

identification requirements to such extremes, in no case may

Vodafone can be accused of negligence or lack of solidity of the measures

taken at this time, but first the rules should be established and

subsequently, where appropriate, penalize the operator that does not apply them, but does



that is not in accordance with the law is to try to use the route directly

penalty as a method of setting security parameters

enforceable.” (The underlining is ours)

The reflections that were made in the opening agreement, which were ratified in the

proposed and reiterated now, are not an attempt by the Agency to "increase" "the

identification requirements incorporating conservation obligations and

technical verification of documents”.

Contrary to what VODAFONE believes, 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 a prepaid service with it in compliance with the

Additional provision of Law 25/2007, in light of articles 5.2, 24 and 25 of the

GDPR.

2.2. Legitimation based on section b) of article 6.1. GDPR.

VODAFONE stated in its allegations to the opening agreement that the treatment

of the claimant's data could be covered by the legal basis of article

6.1.b) of the GDPR: "the treatment is necessary for the execution of a contract in the

that the interested party is a party or for the application at his request of measures

pre-contractual;”

As the defendant recognized in her allegations to the initiation agreement, linked to the contracting the prepaid service processed personal data that did not belong to the purchaser of the prepaid card, but to a third party, to the claimant. So the claimant was not a party to the prepaid service contract.

The legal basis of article 6.1.b) that is invoked as a basis for the legality of the treatment operates with respect to the processing of personal data that is necessary to execute a contract in which the interested party (the owner of the data) has been a party.

Therefore, it is obligatory to conclude that it does not concur in the treatment of the data of the claimant carried out by VODAFONE for this reason for legality, section b) of article 6.1. GDPR.

Nor could the alleged absence of the element of guilt. On this point, we refer to the sections precedents, section 2.1.4.

In view of the foregoing, regarding the processing of personal data of the claimant made by VODAFONE, it is concluded that this entity, as responsible for the treatment, incurred in a violation of article 6.1. of the GDPR, typified in article 83.5.a) GDPR, precept that establishes:

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:

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 offences, it is three years.

Sanction of a fine: Determination of the amount

IV.

Article 58.2 of the GDPR attributes various powers to the control authorities

among those mentioned in section i), the imposition of a fine

administration in accordance with article 83 of the GDPR.

In this case, it is agreed to impose on VODAFONE, as responsible for the

treatment, for the violation of article 6.1 of the GDPR that is attributed to it, a sanction

administrative fine.

In determining the amount of the fine to be imposed, it is necessary to observe the

provisions of articles 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 contemplated in

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

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

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

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

such as the number of interested parties affected and the level of damages that

have suffered;

b) intentionality or negligence in the infringement;

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."

In this case, the concurrence of the following related factors can be seen

in article 83.2 of the GDPR that operate as aggravating circumstances, since they imply a

greater illegality of the conduct or greater guilt of the offending subject.

At the time of examining each of the aggravating circumstances whose concurrence

has been recognized by this Agency, mention will be made, for systematic reasons, of the objections that the defendant has raised against its application.

1.-Article 83.2.a): “the nature, seriousness and duration of the offence, taking into account account the nature, scope or purpose of the processing operation concerned, as well as the number of interested parties affected and the level of damages that they have suffered;

In the factual assumption that we analyze this circumstance has a significance and special relevance that affects, aggravating it, the amount of the fine that must be be imposed, since in it there is room for various aspects of the conduct of the claimed that prove greater illegality and culpability:

(i) The "seriousness of the infringement" taking into account "the level of damages" that the affected person has suffered.



The seriousness of the damages that VODAFONE's conduct has inflicted on the claimant is obvious. His person has been linked to the commission of criminal offenses both in police proceedings and in legal proceedings of a criminal nature (Preliminary Proceedings of criminal proceedings before two bodies jurisdictional). Consequences of enormous importance that derive, uniquely and exclusively, of the conduct of the defendant who, acting with a serious lack of diligence, has breached the principle of legality in the treatment of data personal data collected when contracting a prepaid line.

VODAFONE opposes the application of this circumstance, since it considers that it is not

have caused damages to the claimant given that there is no evidence

proven the existence of patrimonial damages and that the fact that the

claimant has been immersed in police and judicial proceedings is not the result of

the actions of VODAFONE but as a consequence of the fraudulent actions of a

third.

As regards the invoked absence of patrimonial damages, it must be

warn that the RGPD seeks to protect natural persons with regard to the

processing of personal data, in view of the risks that may arise

create such treatment. Therefore, when the risk has materialized into effective damage to the

interested party, this includes any type of damage that is caused to him, not only of

patrimonial nature but also any injury to the rights and freedoms of

interested parties, such as those relating to honor or reputation.

As regards the damages caused to the claimant who

VODAFONE denies having generated, it should be noted that, while VODAFONE

breached the obligations imposed by Law 25/2007 in connection with the regulations

of data protection, it is the cause of the damages suffered by the affected party.

(ii) The "duration of the infringement" taking into account the purpose of the operation of

treatment. The processing of the claimant's personal data was maintained

for more than 15 months.

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 11/28/2019, the date on which

that the defendant registered a prepaid line linked to the data without legitimacy

of the claimant. The personal data of the affected party continued to be processed by

VODAFONE after the deactivation of the service, which dates back to

07/19/2020, as confirmed by the screenshot provided as document 3 in

response to transfer actions (second proven fact). According to the letter

that VODAFONE addresses the claimant, on 03/17/2021 proceeded to cancel their

data.



The defendant opposes the application of this aggravating circumstance and has alleged to sustain

his rejection of these arguments:

a) The Judgments of the National High Court cited are not applicable, since the

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

that do not deal with the protection of personal data, we are dealing with conduct

repeated, conscious and active on the part of the offenders, elements that do not

found in the case of Vodafone.

In response to what was alleged to the contrary, it suffices to indicate that with the sentences

mentioned have not been intended to illustrate any specific issue of protection of

data but to corroborate, through the doctrine of the A.N. and the jurisprudence of the T.S., the

concept of permanent infringement, since the permanent nature of the infringement is

connects in this case with its "duration", which is one of the factors to take into account

to consider the concurrence of the circumstance of article 83.2.a) of the GDPR.

b) VODAFONE invokes that article 83.2 a) of the GDPR establishes that the "duration of the offense" 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 such as the number of interested parties affected and the level of damages that have suffered". However, in this case there is only one affected person, the claimant.

According to article 83.2.a), 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 also the nature, scope or purpose of the processing operation of which try. And the truly relevant aspect with a view to the application of this The circumstance is not -as the defendant maintains- that there is only one affected, but the purpose pursued by the processing operation provided for in the Additional provision Sole of Law 25/2007: articulate mechanisms to control employment for of the mobile telephone equipment acquired through the modality of prepaid (Preamble of Law 25/2007).

With regard to VODAFONE's objection that in the matter under examination there is only one affected -the claimant- it is necessary to refer to the considerations that Extreme do the Guidelines 4/2022, of the European Committee for Data Protection (CEPD), for the calculation of administrative fines in accordance with the GDPR, approved for public consultation purposes on 05/12/2022.

With regard to this factor -the number of interested parties- the Guidelines refer to "the number of specific but also potentially affected stakeholders". They say how much the greater the number of stakeholders involved, the more weight you can attribute to this factor the supervisory authority. They warn that, in many cases, it can also be considered that the infringement adopts "systemic" connotations and, therefore, can affect, even at different times, to other interested parties who have not submitted

claims or reports to the control authority. The supervisory authority may,

depending on the circumstances of the case, consider the relationship between the number of

affected stakeholders 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

systemic character. The greater the number of stakeholders involved, the more weight



The supervisory authority may attribute to this factor. The original version of the Guidelines

4/2022, in English, address this issue in paragraph 54 point 4.

c) Law 25/2007 (Sole Additional Provision in relation to its article 5) imposes on

VODAFONE the obligation to collect and keep "the name, surname and nationality

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

used [...]".

Said affirmation of the defendant is distorted by what is stated in the Foundation

Legal precedent regarding the offense at hand, since the treatment

carried out was not covered by the precepts alleged to the contrary

2.- Article 83.2.d) GDPR: "The degree of responsibility of the person in charge or of the

processor, taking into account the technical or organizational measures that

applied by virtue of articles 25 and 32;".

The defendant has limited herself to declaring that the third party that contracted with her exceeded the

company security policy but without providing any evidence to demonstrate

that he obtained from the person who intervened in the contracting a document that

certify that he was indeed the owner of the data that he had provided as

own or that articulated some mechanism that would allow verifying the veracity of the identity data provided. While the defendant has not been able to prove neither extreme on this issue is unknown what organizational measures had implemented and if these were correct and necessary taking into account the current technical development and the evident risk that the contracting of the services that the claimed entity markets represents for the rights and freedoms of people.

The defendant rejects the application of this aggravating circumstance and alleges:

"In order to avoid unnecessary repetition, we refer to what is stated in the First Allegation in relation to the suitability of requesting the DNI or the Passport to prove the identity of the applicant. In any case, and as we have already pointed out, the Initiation Agreement is related to the alleged infringement of article 6.1 of the GDPR, not to the security measures adopted by Vodafone."

In response to VODAFONE's allegation to reject the application as an aggravating circumstance of the circumstance of section d) of article 83.2., we refer to the Foundation Legal precedent. It is convenient to insist once more that the principle of proactivity means transferring to the data controller the obligation, not only to comply with regulations, as well as being able to demonstrate compliance. Between the mechanisms that the GDPR contemplates to achieve this are those provided for in the Article 25, "data protection by design", according to which the person responsible must apply "both at the time of determining the means of treatment and in the time of the treatment itself" technical and organizational measures that guarantee that makes an effective application of the principles of the GDPR on the occasion of the treatments you do.

The presentation on the protocol that VODAFONE follows to verify compliance of the principles of data protection shows that he had not applied any

measure that responds to the provisions of article 25 of the GDPR, which is why

considers that the circumstance of article 83.2.d) exists as an aggravating circumstance.

3.- Article 83.2.e) GDPR: "Any previous infringement committed by the person in charge or the

treatment manager".

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, -whether by reason of the legal nature of the infringement, by the

infringed precept, or for the time elapsed since its commission or from the

imposition of the sanction - on the set of infractions committed by a

responsible or in charge of treatment.

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

attention to the nature, seriousness and duration of the infringement, to its nature

intentional [...] or any pertinent infraction [...]". (The underlining is ours)

Recital 148 does introduce a delimitation in the group formed by the

all of the infractions of a person in charge or in charge of treatment, since it urges

to pay special attention to any "relevant" violations. Term that responds to

the translation of the adjective "relevant" that appears in the original text in English and that

It means pertinent or relevant.

It is therefore considered 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 this sense, the resolutions issued by the AEPD have been cited 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

The history of infractions of the defendant, 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 who provided

as his personal data of which he was 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.

When the events occurred in which the current infringement of article

6.1. GDPR, the defendant was fully aware of the deficiencies it suffered from

its security policy to comply with the obligations imposed by the GDPR in

relation to the principle of legality and the principle of proactivity. resolutions

sanctions that are mentioned should have been an additional reason to review

the protocols that it has established to verify the identity of clients with

occasion of contracting the products or services that it sells.

VODAFONE does not agree with what has been considered antecedents

"pertinent" and rejects the application as an aggravating circumstance of the article

83.2.e) of the GDPR. He is of the opinion that the procedures mentioned - cited in the

initial agreement and reiterated in the proposal - dealt with assumptions of fact

different from the one that concerns us now, since in them the third parties who posed as

the claimants contracted products "on behalf of the claimants" and the latter

received the corresponding invoices, something that has not happened now.

VODAFONE's claim cannot prosper either. These details are enough:

first, that, as has been pointed out regarding this circumstance, the literalness of the

precept - "Any previous infraction committed by the person in charge or in charge of the

treatment"- is extraordinarily broad and does not make any limitation, so

a literal interpretation would have led to framing any infringement of the

data protection regulations for which the defendant had been penalized.

The AEPD has interpreted this provision restrictively and has restricted its

application to those infractions that suppose a "pertinent precedent" 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 a systematic interpretation of

that standard and a very different one, what VODAFONE intends. Pretend you can't

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" between the

facts on which the infractions for which she was penalized in the

past and the facts that concern us. However, as explained, the

relevance of the precedents that have been mentioned derives from the fact that, in them,

As in the case presented here, VODAFONE had not adopted measures in

application of article 5.2, in relation to 5.1.a and 6.1; 24 and 25 of the GDPR.

4.- 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 that of

specially protected data regulated by article 9 of the GDPR - recital 51

of the GDPR- and, in addition, many other data not included in that precept. He

recital 75 mentions in detail the personal data whose processing may

entail a risk, of varying severity and likelihood, to the rights and

freedoms of natural persons as a consequence of the fact that they can cause damage

and physical, material or immaterial damages. 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 confidentiality of

data subject to professional secrecy, unauthorized reversal of pseudonymization or

any other significant economic or social harm;”

Through the passport number the natural person is identified in a way

unquestionable unless proven otherwise. The quality attributed to this data

becomes particularly sensitive as long as, if your treatment does not go

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.

In the case examined, the unlawful treatment carried out by the defendant fell

about a particularly sensitive personal data of the claimant: the number of his

passport, which affects the seriousness of VODAFONE's conduct, having to

assess the concurrence, as an aggravating circumstance, of the circumstance of section g)

of article 83.2. GDPR.

The defendant rejects his estimate as an aggravating circumstance, which he justifies as follows:

The Agency considers that, in accordance with the provisions of Recital 75 of the

GDPR, the passport number would be "particularly sensitive data insofar as

how much a third party can impersonate the identity of a natural person with total

ease, with the risks that this entails for privacy, honor and the

patrimony of the supplanted".

In these cases, the usurpation of identity occurs prior to the

contracting the prepaid line, that is: contracting the prepaid line is a

consequence of the identity theft, not the identity theft itself

same considered. In other words, it is not that Vodafone with its conduct has facilitated

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

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

Vodafone.

On a purely theoretical level, the Agency's reasoning could reach

be admitted if the sanctioned party is responsible for conserving and preserving the security

the personal data of the data subject and, due to deficient security measures,

would allow a third party to gain illegitimate access to said data and, with this,

could impersonate the identity of the affected party. It is not the case." (The underlining is ours)

In response to what was alleged by the defendant against the application as an aggravating circumstance

of the circumstance of section g) of article 83.2 of the GDPR, we must insist on

once more in the principle of proactive responsibility and in the obligations that

to the controller, in this case to VODAFONE. Regarding the allegation of

that "there has not been an identity theft" it should be noted that when the

recital 75 of the GDPR refers to the fact that data processing "may give rise to

problems of discrimination, identity theft or fraud," you are not using the

terms identity theft and fraud in a legal technical sense, that is, as

conducts that meet the requirements to be subsumed in a criminal offense contemplated

in the Spanish Penal Code. With regard to VODAFONE's statement that

there was no identity theft, we understand that with it he is referring to

that the type of article 401 of the Spanish Criminal Code is not met, which is true.

However, the GDPR is a rule applicable to all member states of the

Union whose legal systems, with the exception of the regulations of the U.E. that

links them, they are disparate, even more so when conducts classified as criminal

is concerned, so it seems clear that the Community legislature did not use those

Expressions with the legal technical meaning that the defendant wants to give them.



Lastly, regarding VODAFONE's comment according to which "On a plane

purely theoretical, the Agency's reasoning could be accepted if the

sanctioned was the person responsible for conserving and preserving the security of the data

personal data of the data subject [...]", it should be remembered, on the one hand, that the person responsible for the

treatment, condition that the claimed party has regarding data processing

that is the object of assessment in this file, is obliged to comply with the

principles that govern the treatment and to be in a position to prove their

compliance. On the other, that in accordance with article 4.2 of the GDPR, it is understood by

"processing" "any operation or set of operations performed on data

personal data or sets of personal data, either by procedures

automated or not, such as the collection, registration, organization, structuring,

conservation, adaptation or modification, extraction, consultation, use,

communication by transmission, diffusion or any other form of authorization of

access, collation or interconnection, limitation, deletion or destruction".

5.- Article 83.2.k) RGPD, in relation to 76.2.b) LOPDGDD: "The connection of the

activity of the infringer with the processing of personal data".

The link between the business activity of the defendant and the data processing

personal is evident and intense. In the development of the activity that is his own, the

claimed needs to process personal data on a regular basis, which affects

in the diligence that should be demanded of him in compliance with the principles that govern

the processing of personal data and the quality and effectiveness of the measures

technical and organizational that must be implemented to guarantee respect for

this fundamental right of both its clients and third parties.

Attenuating:

VODAFONE has requested the application as a mitigation of the circumstance collected

in article 83.2.b): lack of intentionality or negligence. However, this

The claimed party's claim must be rejected for obvious reasons. we refer

to the exposure included in the preceding Basis, section 2.1.

In consideration of the foregoing, valued the circumstances whose concurrence

as aggravating circumstances, -paragraphs a), d), e) g) and k) of article 83.2 of the

GDPR- It is agreed to penalize VODAFONE for the violation of article 6.1. of the

GDPR, typified in article 83.5.a) of the GDPR, with an administrative fine for

amount of €100,000.

V

On the transfer of the claimant's data to the Civil Guard and the treatment that

this has performed as judicial police on the occasion of the actions of

investigation.

Finally, given that the claim that gave rise to this file

sanctioner also mentioned that the defendant had transferred the personal data

of the claimant to the Civil Guard and that this security body, as

As a result of the personal data provided by VODAFONE, it carried out the

identification of the claimant in the framework of the investigation actions



related to fraud committed through Wallapop, it is appropriate to make the

The following precision was also made in the agreement to initiate this procedure:

That the communication of personal information concerning the claimant that

VODAFONE carried out the Civil Guard, acting that State security body

in functions of the Judicial Police, in the course of some Investigative Proceedings, it is

a lawful treatment of the personal data of the claimant who has his

legal basis in article 6.1.c) of the GDPR - "the processing is necessary to

compliance with a legal obligation applicable to the data controller”- in

connection with article 4.1 of Organic Law 2/1986, of March 13, on Forces and

State Security Corps, which provides that "Everyone has the duty to provide

to the Security Forces and Corps the necessary assistance in the investigation and

prosecution of crimes in the terms provided by law.”

In turn, the processing of the personal data of the claimant who made the

Civil Guard - data that it collected and obtained in the development of its activity of

investigation of allegedly criminal conduct - is not governed by the GDPR but by

Directive (EU) 2016/680 and the rule of transposition into domestic law, constituted

currently by Organic Law 7/2021, of May 26, on data protection

personal data processed for the purposes of prevention, detection, investigation and prosecution

of criminal offenses and execution of criminal sanctions. when they happened

the facts - the Civil Guard's request to VODAFONE for personal data

linked to the controversial line and their response dates from 03/10/2020 and

03/13/2020, respectively- the applicable internal regulation was Organic Law 15/1999,

of personal data protection (LOPD), in particular its article 20.2 -in

application of the fourth Transitory Provision of the LOPDGDD- which established that

“The collection and treatment for police purposes of personal data by the

Security Forces and Corps without the consent of the affected persons are

limited to those assumptions and categories of data that are necessary for the

prevention of a real danger to public safety or to the repression of

criminal offences”.

Therefore, the treatment in which the communication to the Civil Guard of

the personal data of the claimant that appeared in the systems of the claimant

linked to the controversial line, a communication that was made within the framework of the

investigations that this security body carried out in the context of some

Preliminary investigation proceedings of criminal offenses, and the treatment that

Civil Guard would have made such data for the same purpose, it was adjusted to

Right without there being evidence of administrative infraction in these conducts.

Therefore, in accordance with the applicable legislation and assessed the criteria of

graduation of sanctions whose existence has been accredited,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE VODAFONE ESPAÑA, S.A.U., with NIF A80907397, for a

infringement of article 6.1 of the GDPR, typified in article 83.5.a) of the GDPR, a

administrative fine of €100,000 (one hundred thousand euros)

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

THIRD: Warn the penalized person that they must make the imposed sanction effective

Once this resolution is enforceable, in accordance with the provisions of Article

Article 98.1.b) of Law 39/2015, of October 1, on Administrative Procedure

Common of Public Administrations (hereinafter LPACAP), within the payment period

voluntary established in article 68 of the General Collection Regulations,

approved by Royal Decree 939/2005, of July 29, in relation to article 62 of

Law 58/2003, of December 17, through its entry, indicating the NIF of the

sanctioned 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

C / Jorge Juan, 6

28001 – Madrid

938-120722

www.aepd.es

sedeagpd.gob.es



Director of the Spanish Data Protection Agency

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es