 File No.: PS/00496/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: D.A.A.A. (hereinafter, the complaining party) dated May 17,

2021 filed a claim with the Spanish Data Protection Agency. The

The claim is directed against Working Capital Management España, S.L. with NIF

B86878121 (hereinafter the claimed party or WCM).

The grounds on which the claim is based are as follows.

The claimant states that he has been aware of the inclusion of his data

information in common credit information systems by the entity

claimed, a company with which he has never made any contract.

It adds that said inclusion was motivated by the non-payment of a loan to NBQ

Technology, S.A.U. (hereinafter NBQ), which he did not hire, for which he states that he has

been a victim of identity theft.

On the other hand, he indicates that NBQ informs him that the credit was assigned on December 23

2020 to the entity Quartz Capital Fund S.C.A., being Working Capital Management

Spain, S.L. the person in charge of the treatment, not having proof of having received

no communication about it.

And, it provides, to justify the facts, the following documentation:

- Complaint filed with the police on December 23, 2020, in relation to

identity theft to contract a loan.

- Complaint filed with the police for the theft of his wallet, from the year 2018.

- Request for deletion addressed to the respondent dated March 22,

2021 and acknowledgment of receipt on the 30th of the same month and year.

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5

December, of Protection of Personal Data and guarantee of digital rights (in

hereinafter LOPDGDD), said claim was transferred to the claimed party, to

to proceed with its analysis and inform this Agency within a month of the

actions carried out to adapt to the requirements set forth in the regulations of

Data Protection.

On July 15, 2021, this Agency received a response letter

stating that they attach as Annex I, a copy of the answering brief

sent on July 15, 2021 to the interested party, via email, which is the one that appears in the

“loan contract”, which is attached as Annex IV.

That WCM cannot report the causes that originally motivated the

claim, without prejudice to the fact that it is estimated that this could be in the non-connection of the

interested party between the original NBQ creditor and the assignee creditor; that is, WCM, to

despite the fact that this would have been brought to his attention, on the occasion of the acquisition

of the aforementioned debt (Annexes IV, V and VI).

That WCM is endowed with convenient procedures to attend to the exercise of

rights of any interested party, as established by the legal system.

(This procedure is attached as Annex II).

THIRD: On October 6, 2021, the Director of the Spanish Agency for

Data Protection agreed to admit for processing the claim presented by the party

claimant.

FOURTH: On November 19, 2021, the Director of the Spanish Agency

of Data Protection agreed to initiate a sanctioning procedure against the claimed party,

in accordance with the provisions of articles 63 and 64 of Law 39/2015, of October 1,

of the Common Administrative Procedure of the Public Administrations (in

hereinafter, LPACAP), for the alleged violation of Article 6.1 of the RGPD, typified in

Article 83.5 of the RGPD.

FIFTH: Having been notified of the aforementioned initiation agreement, the party complained against submitted a written

allegations in which, in summary, it stated: “that the transfer of data

property of the debtor (the claimant in this case), which occurred as

consequence of the transfer of credits, did not require the prior consent of the

debtor as the owner of their personal data, since the regulations with a range of

Law that regulates the transfer of credits clearly establishes that the consent

of the debtor is not necessary for the valid transmission of a credit (nor is its

knowledge, without prejudice to the release effect on payments), and said assignment must

of data also be considered valid under article 8.1 of the RGD.

It is possible to additionally allege the protection that for my company establishes the current art.

21 of the LOPDGDD.

We also understand that there is another legitimate reason for the transfer of data.

in a credit assignment, and it is none other than the existence of an interest

legitimate (article 6.1.f) of the RGPD).

In relation to the inclusion of the personal data of the claimant (the debtor, in this

case) in common credit information systems, this Agency assigns

erroneously to my company the authorship of such inclusion, as well as its maintenance

negligent in such systems.

On the one hand, as can be seen in the attached NBQ certification

proceeds to register the data in the Asnef file dated 02/06/2020. Subsequently

there is a portfolio change in favor of the Working entity on 12/23/2020.

Consequently, my company cannot be attributed the authorship or the request for the

registration of the debt and debtor (the person of the claimant).

On the other hand, as can be verified in the certification attached to this

pleadings brief, also issued on November 30, 2021 by

Equifax, data reported by Working does not appear, whose discharge date was

05/25/2021”

FIFTH: On January 10, 2022, the testing period began,

remembering: 1. Consider reproduced for evidentiary purposes the complaint filed

by the claimant and their documentation, the documents obtained and generated that

are part of the file and 2. Consider reproduced for evidentiary purposes, the

allegations to the initiation agreement of PS/00496/2021, presented by the entity

reported.

SIXTH: On January 31, 2022, a resolution proposal was formulated,

proposing That the Director of the Spanish Data Protection Agency

sanctions Working Capital Management España, S.L. with NIF B86878121, for a

infringement of Article 6.1 of the RGPD, typified in Article 83.5 a) of the RGPD, a

fine of €40,000.00 (forty thousand euros).

The party complained against presented arguments to the Resolution Proposal, in which

reiterates in the exposed arguments that, in summary, it states: “that it has acted in

absolutely diligent manner and the basis of its treatment is absolutely lawful

consisting of the fulfillment of its contractual obligations. Upon receipt of the request

by the claimant, the respondent contacted NBQ Technology, S.A., to

request this merchant to review the documentation in its possession of the

contract in question.NBQ Technology, S.A. never told us that

acknowledge that the contracting process in the case of the claimant was fraudulent,

It is noteworthy that the only proof of this is the complaint filed by the

complainant to the police.

Notwithstanding the foregoing, and following a criterion of prudence, the respondent decided to

verisimilitude to the version of the claimant and access to the requested data deletion

for this and the cancellation of your loan. It is true that it exceeded 25 days of the

deadline to do so, but this is justified by the consultations that he had to make to the

transferor to review the documentation of the contracting file.

That the complaint filed by the claimant coincides in time with the date of

granting of the deed of sale of the loan portfolio.

On December 23, 2020, he acquired a credit of ownership of today

claimant.

That this organization, complying with the provisions of article 14 RGPD, sent

communication to the now claimant, informing him of the acquisition of the

credit, origin of the same, and how this organization would treat from now on its

data.

It should be noted that together with the right of suppression, a copy of all the

documents in which this organization processes user data:

Letter communicating the transfer of credit.

Loan agreement signed with the company NBQ Fund One S.L., along with a table

of amortizations.

Request the file of these actions or subsidiarily Warning, and

proceed to graduate and attenuate the reported infraction according to the provisions of the

art. 83.2 RGPD, understanding that there has been no illicit treatment of

in accordance with article 6 of the RGPD".

Of the actions carried out in this procedure and the documentation

in the file, the following have been accredited:

PROVEN FACTS

FIRST. - It is stated that your data, as stated by the complaining party in its

claim, have been used for the fraudulent contracting of a loan without

Your consent.

SECOND. - Contained in the deed of sale and transfer of credits No. 5120, of the

protocol of the Barcelona notary D. B.B.B., granted on 12/23/2020, by means of

that the claimed party (assignee) acquires the loan portfolio from the NBQ merchant

(assignor), of which the debt claimed from the claimant is part.

THIRD. - It is accredited in the certificate issued by the company Equifax Ibérica, S.L.

(managing entity of the Asnef file) dated November 30, 2021, that the change

portfolio in favor of the entity WCM was carried out on 12/23/2020.

The date of registration by NBQ (assignor) is recorded as 02/06/2020 and for a debt amount

XXX.XX euros.

FOURTH. - In the certificate issued by Equifax Ibérica, S.L. dated 30 of

November 2021, it is stated that the date of removal in the Asnef file of the part

claimant, it was 05/25/2021.

FIFTH. - There is evidence of the complaint filed with the General Directorate of the Police, dependency: Burjasot-Godella, certificate: 5281/20, on December 23, 2020, in relation to identity theft for contracting a loan.

SIXTH. - The request for deletion addressed to the claimed party dated 22 March 2021 and acknowledgment of receipt on the 30th of the same month and year.

FOUNDATIONS OF LAW

Yo

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

The Director of the Agency is competent to resolve this procedure.

Spanish Data Protection, in accordance with the provisions of art. 58.2 of the RGPD and in the art. 47 and 48.1 of LOPDGDD.

II

The defendant is charged with the commission of an infringement due to infringement of Article 6 of the RGPD, “Legality of the treatment”, which indicates in its section 1 the assumptions in which the processing of third party data is considered lawful:

"1. The treatment will only be lawful if it meets at least one of the following conditions:

a) the interested party gave their consent for the processing of their data personal for one or more specific purposes;

b) the treatment is necessary for the execution of a contract in which the interested party is a party or for the application at the request of the latter of measures

pre-contractual;

c) the treatment is necessary for the fulfillment of a legal obligation

applicable to the data controller;

d) the treatment is necessary to protect the vital interests of the interested party or of

another natural person;

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

public interest or in the exercise of public powers vested in the controller

of the treatment;

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

pursued by the data controller or by a third party, provided that

over said interests do not prevail the interests or the rights and freedoms

fundamental data of the interested party that require the protection of personal data,

in particular when the interested party is a child. The provisions of letter f) of

The first paragraph will not apply to the treatment carried out by the

public authorities in the exercise of their functions.

The infringement is typified in Article 83.5 of the RGPD, which considers as such:

"5. Violations of the following provisions will be sanctioned, in accordance

with section 2, with administrative fines of a maximum of EUR 20,000,000 or,

in the case of a company, an amount equivalent to a maximum of 4% of the

global total annual turnover of the previous financial year, opting for

the largest amount:

a) The basic principles for the treatment, including the conditions for the

consent under articles 5,6,7 and 9."

The Organic Law 3/2018, on the Protection of Personal Data and Guarantee of the Digital Rights (LOPDGDD) in its article 72, under the heading "Infringements considered very serious" provides:

"1. Based on the provisions of article 83.5 of the Regulation (U.E.) 2016/679 are considered very serious and the infractions that suppose a substantial violation of the articles mentioned in it and, in particularly the following:

(…)

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

III

In accordance with the available evidence, it is considered that the claimed party violated Art. 6.1 of the RGPD, since when the party claimant became aware that their personal data was included in the Asnef file, contacted the claimed party on March 22, 2021, where he denounces that he has been the object of a contracting fraud and files complaint to the National Police, and it is stated that said shipment was delivered in proof of postal service delivery on March 30, 2021

Well, on December 23, 2020, the loan was assigned through Contract for the Sale and Assignment of the Portfolio to the claimed party. So with date March 30, 2021, was aware of these facts, however, he did not acted and continued to process the data of the complaining party without legitimate basis for this, until May 25, 2021, the date on which WCM terminated the part

claimant in the Asnef file, contravening the requirements set out in the

LOPDGDD.

In relation to the allegations made by the respondent, it is necessary to

state that article 20.1 b) of the LOPDGDD establishes: "that the data is

refer to certain debts, due and payable, whose existence or amount had not been

been the subject of an administrative or judicial claim by the debtor or through a

binding alternative dispute resolution procedure between the parties".

Therefore, we can consider that the respondent party has acted without the

due dilegence.

Due diligence is attention to the legal duty of care. Be

due diligence implies, in terms of that legal duty of care, to prevent the

materialization of the risk (identity theft) establishing with character

in advance of treatment, an effective system of appropriate measures to prevent it; such

system must be constantly evaluated. As the jurisprudence affirms, the

responsibility derives from the actions of those who are responsible for being diligent

and "cannot be considered excluded or attenuated by the fact that the

possible fraudulent action of a third party, since the responsibility of the plaintiff

It does not derive from his actions, but from his own".

Accordingly, due diligence is made up of four elements:

identify (assessment of the actual and potential impact of data treatment activities)

data); prevent, mitigate (through follow-up and monitoring) and, finally, render

accounts (communicating how you deal with negative consequences

of improper data processing). And all this, within a continuous process.

Due diligence, which must be appropriate to the business environments in which

that the person in charge of the treatment moves, includes not only the adoption of

technical and organizational measures appropriate to the treatment in question, but the

ability to prove compliance.

Therefore, the data controller must “be obliged to apply

timely and effective measures and must be able to demonstrate the conformity of the

processing activities with this Regulation, including the effectiveness of the

measures. Such measures must take into account the nature, scope, context and

the purposes of the treatment, as well as the risk to the rights and freedoms of the

natural persons”, considering 74 of the RGPD.

Demonstrating due diligence is essential, not being enough

allege the absence of guilt, because as affirmed by the National High Court, for all the

Judgment 278/2015 of June 30, 2015 (Rec. 163/2014), "In view of the foregoing,

be added, following the judgment of January 23, 1998, partially transcribed in the

SSTS of October 9, 2009, Rec 5285/2005, and of October 23, 2010, Rec

1067/2006, that "although the culpability of the conduct must also be subject to

test, must be considered in order to assume the corresponding load, which

ordinarily the volitional and cognitive elements necessary to appreciate

they are part of the typical behavior tested, and that their exclusion requires that

the absence of such elements is proven, or in its normative aspect, that it has been

used the diligence that was required by the person who alleges its non-existence; not enough, in

sum, for the exculpation in the face of a typically unlawful behavior the

invocation of the absence of guilt".

In conclusion, in order to act with due diligence, the person responsible for the

treatment must comply with the RGPD and the LOPDGDD and establish in advance

adequate mechanisms to verify the identity of the people whose data

personal is going to treat or treats (if it is subsequently detected, during the

treatment, an identity theft), to ensure, ultimately, that

holds legitimacy to process such personal data.

In accordance with the available evidence, it is estimated that the

conduct of the claimed party violates article 6.1 of the RGPD being constitutive of

the infraction typified in article 83.5.a) of the aforementioned Regulation 2016/679.

The documentation in the file offers evidence that the party

claimed, violated article 6.1 of the RGPD, since it carried out the treatment of the

personal data of the complaining party without their consent. Personal information

of the complaining party were incorporated into the information systems of the

company, without having proven that he had his consent for the

collection and further processing of your personal data.

It must be remembered that when the complaining party became aware that his

personal data were included in the Asnef file, he contacted

with the claimed party, on March 22, 2021, where he denounces that he has been

of a contracting fraud and files a complaint with the National Police, and there is evidence

delivered said shipment to WCM on proof of delivery of the postal service on the 30th of

March 2021, however, did not act and continued to process the data of the part

claimant without legitimate basis for it.

Therefore, we can consider that the respondent party has acted without the

due dilegence.

In this sense, the Contentious-Administrative Chamber of the Court

Supreme Court, in its judgment of December 13, 2021, confirming the Judgment of

the National Court of March 13, 2020, indicates in relation to a sanction

imposed for fraudulent contracting derived from identity theft, which

that led to the improper inclusion of the interested party in a file of defaulters, exposes

"…we share the opinion of the Chamber of the National High Court regarding the

insufficiency of the measures applied by the appellant in the

hiring. To the considerations set forth in the judgment under appeal, which

we share and make our own, we will only add two observations:

First, the verification measures applied by the appellant

seem entirely aimed at ensuring the good end of the loan, but, in

Instead, they entirely disregard the objective of verifying the truth and accuracy

of the data, and, in particular, to verify that the person requesting the credit is

precisely who he claims to be. Thus, in any case in which a third party

improperly use a stolen or lost DNI to make a purchase or

request a credit online, the non-consensual treatment of the

personal data of the holder of the document, even if he had denounced at the time

before the authorities the loss or theft of your DNI, since none of the measures

enunciated by the appellant appears minimally oriented to prevent or hinder

for that result to occur.

Secondly, the foregoing does not mean that it is placed on the company

contracting party the responsibility to prevent the occurrence of an illegal or criminal act

such as the fraudulent use of a DNI by someone who is not its owner. But yes

is required of said contracting company, as a necessary diligence so that it is not

may reproach the breach of its obligations in terms of protection of

personal data - both in regard to the requirement of consent

of the interested party as in relation to the principle of veracity and accuracy of the data- the

implementation of control measures aimed at verifying that the person who intends to

hiring is who they say they are, that is, who coincides with the holder of the DNI provided".

Respect for the principle of legality that is in the essence of the fundamental right

of protection of personal data requires that it be accredited that the

responsible for the treatment displayed the essential diligence to prove that

extreme. Failure to act in this way -and this Agency, who is responsible for ensuring

for compliance with the regulations governing the right to data protection of

personal character - the result would be to empty the content of the principle of legality.

The lack of diligence displayed by the entity in complying with the

obligations imposed by the personal data protection regulations

it is therefore evident. Diligent compliance with the principle of legality in the treatment

of third-party data requires that the data controller be in a position

to prove it (principle of proactive responsibility).

IV

In accordance with the provisions of the RGPD in its art. 83.1 and 83.2, when deciding the

imposition of an administrative fine and its amount in each individual case will be

taking into account the aggravating and mitigating factors listed in the article

indicated, as well as any other that may be applicable to the circumstances of the

case.

“Each control authority will guarantee that the imposition of fines

administrative actions under this article for violations of this

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

effective, proportionate and dissuasive.”

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

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

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

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

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

nature, scope or purpose of the processing operation in question

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

damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor

to alleviate the damages suffered by the interested parties;

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

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

applied under articles 25 and 32;

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

treatment;

f) the degree of cooperation with the supervisory authority in order to put

remedying the breach and mitigating the possible adverse effects of the breach;

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

h) the way in which the supervisory authority became aware of the infringement,

in particular if the person in charge or the person in charge notified the infringement and, in such

case, to what extent;

i) when the measures indicated in article 58, paragraph 2, have been

previously ordered against the person in charge or the person in charge in question

in relation to the same matter, compliance with said measures;

j) adherence to codes of conduct under article 40 or mechanisms

certificates approved in accordance with article 42, and

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

case, such as financial benefits realized or losses avoided, direct

or indirectly, through infringement."

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

"Sanctions and corrective measures", provides:

"two. In accordance with the provisions of article 83.2.k) of Regulation (EU) 2016/679

may also be taken into account:

a) The continuing nature of the offence.

b) The link between the activity of the offender and the performance of treatments

of data

personal.

c) The profits obtained as a result of committing the offence.

d) The possibility that the conduct of the affected party could have induced the

commission

of the offence.

e) The existence of a merger by absorption process after the commission

infringement, which cannot be attributed to the absorbing entity.

of the

f) Affectation of the rights of minors.

g) Have, when it is not mandatory, a delegate for the protection of

data.

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

voluntary, to alternative conflict resolution mechanisms, in those

assumptions in which there are controversies between those and any interested party."

In accordance with the precepts transcribed, in order to set the amount of the

sanction of a fine to be imposed in the present case for the infraction typified in the

article 83.5.a) of the RGPD for which the claimed party is responsible, they are estimated

concurrent the following factors:

As aggravating criteria:

-

That the facts object of the claim are attributable to a lack of diligence

of the claimed party (article 83.2.b, RGPD), the claimed party when it had

knowledge of the fraud did not act and continued to process the claimant's data

-

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

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

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

The balance of the circumstances contemplated in article 83.2 of the RGPD, with

Regarding the infraction committed by violating what is established in article 6, it allows establishing

a fine of 40,000 euros (forty thousand euros).

Therefore, in accordance with the applicable legislation and having assessed the criteria for graduation of the sanctions whose existence has been proven, the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE WORKING CAPITAL MANAGEMENT ESPAÑA, S.L. with NIF B86878121, for an infringement of Article 6.1 of the RGPD, typified in Article 83.5 of the RGPD, a fine of €40,000 (forty thousand euros).

SECOND: NOTIFY this resolution to WORKING CAPITAL MANAGEMENT ESPAÑA, S.L.

THIRD: Warn the sanctioned party that he must make the imposed sanction effective once Once this resolution is enforceable, in accordance with the provisions of the art. 98.1.b) of Law 39/2015, of October 1, on Administrative Procedure Common Public Administrations (hereinafter LPACAP), within the payment term voluntary established in art. 68 of the General Collection Regulations, approved by Royal Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003, of December 17, through its entry, indicating the NIF of the sanctioned and the number of procedure that appears in the heading of this document, in the account restricted number ES00 0000 0000 0000 0000 0000, opened on behalf of the Agency Spanish Department of Data Protection in the banking entity CAIXABANK, S.A.. In case Otherwise, it will be collected in the executive period.

Received the notification and once executed, if the date of execution 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 month or immediately after, and if

between the 16th and last day of each month, both inclusive, the payment term

It will be until the 5th of the second following month or immediately after.

In accordance with the provisions of article 50 of the LOPDGDD, this

Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure 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 reconsideration before the

Director of the Spanish Agency for Data Protection within a month from

counting 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 in article 46.1 of the

aforementioned Law.

Finally, it is pointed out 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 by

writing addressed to the Spanish Agency for Data Protection, presenting it through

Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-

web/], or through any of the other registers 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 within a period of two months from the day following the notification of this resolution would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es