 Procedure No.: PS/00126/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

the following:

BACKGROUND

FIRST: D.A.A.A. (hereinafter, the claimant) on July 21, 2020 filed

claim before the Spanish Data Protection Agency. The claim is directed

against CREATOR ENERGY, S.L., with NIF B67301036 (hereinafter, the claimed party).

The claimant expresses the use of their personal data without their consent to

contract at your home the supplies of gas, electricity, in addition to a service of

maintenance called Servielectric Xpress. These contracts were discharged by

the claimed.

SECOND: In accordance with the mechanism prior to the admission for processing of the

claims made before the AEPD, provided for in article 65.4 of the Law

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

digital rights (hereinafter, LOPDGDD), which consists of transferring the

same to the Data Protection Delegates designated by those responsible or

in charge of the treatment, or to these when they have not been designated, and with the purpose

indicated in the aforementioned article, the claim was transferred to the respondent on the 18th and 29th

September 2020, through the electronic notification service and the service

post office, to proceed with its analysis and provide a response within a month.

Being the same returned on September 29 and October 6, 2020. It was not received

response in this Agency by the claimed party.

THIRD: On October 28, 2020, after analyzing the documentation that was

in the file, a resolution was issued by the director of the AEPD, agreeing not to admit

to process the claim. The resolution was notified to the claimant on the 28th of

October 2020, through the Citizen Folder, according to confirmation of receipt

that appears in the file.

FOURTH: On November 6, 2020, the claimant files an optional appeal

of replacement through the Electronic Register of the AEPD, against the resolution relapsed in

file E/06596/2020, in which it shows its disagreement with the resolution

challenged, and provides new documentation and new facts, stating that on the part

of the claimed, responsible for the collection of their personal data and treatment of the

Without their consent, no information or clarification has been received.

Consequently, the director of the AEPD resolves on March 10, 2021,

estimate the replacement resource.

FIFTH: On April 16, 2021, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the claimant, for the

alleged infringement of Article 6.1.b) of the RGPD, typified in article 83.5 a) of the RGPD

and considered very serious in 72.1.b), for prescription purposes, setting a sanction

initial 6,000 euros (six thousand euros).

SIXTH: Having been notified electronically, the start agreement. being the date

of making available on April 16, 2021 and the date of automatic rejection on the day

27 of the same month and year.

SEVENTH

: Formal notification of the start agreement, the one claimed at the time of the

This resolution has not submitted a brief of allegations, so the following is applicable:

indicated in article 64 of Law 39/2015, of October 1, on the Procedure

Common Administrative Law of Public Administrations, which in its section f) establishes

that in case of not making allegations within the stipulated period on the content of the agreement

of initiation, it may be considered a resolution proposal when it contains a

precise pronouncement about the imputed responsibility, for which we proceed to

dictate Resolution.

In view of everything that has been done, by the Spanish Agency for the Protection of

Data in this procedure are considered proven facts the following:

FACTS

FIRST: It is stated that the claimed party used the personal data of the claimant to

contract gas and electricity supplies, as well as a maintenance service

called Servielectric Xpress, not requested by the claimant.

SECOND: It is verified that said contracts were registered by the defendant.

THIRD: It is stated that the respondent did not respond to this Agency, after the requirements

made on September 18 and October 6, 2020.

FOURTH: On April 16, 2021, this sanctioning procedure was initiated for the infraction

of article 6.1.b) of the RGPD, being notified on the 27th of the same month and year. Nope

having made allegations, the respondent, to the initial agreement.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each authority

of control, and according to what is established in articles 47 and 48 of the LOPDGDD, the Director of

The Spanish Agency for Data Protection is competent to initiate and resolve

this procedure.

II

Article 6 of the RGPD, "Legality of the treatment", details 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 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 a party or for the application at the request of the latter of measures pre-contractual;

(…)"

The infraction for which the claimed entity is held responsible is typified in article 83 of the RGPD that, under the heading “General conditions for the imposition of administrative fines”, states:

"5. Violations of the following provisions will be sanctioned, in accordance with section 2, with administrative fines of a maximum of 20,000,000 Eur or, in the case of of a company, of an amount equivalent to a maximum of 4% of the turnover global annual total of the previous financial year, choosing the highest 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 Regulation (EU) 2016/679,

considered very serious and will prescribe after three years the infractions that suppose a

substantial violation of the articles mentioned in it and, in particular, 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 the present case, it is important to point out that if the contracting

fraudulent use of a product and the consent to execute said contract has been

provided by a person other than the owner of the data (identity theft), not

we can understand that there is contractual consent on the part of the latter, that

is harmed.

In legal terms, we can consider that in this situation of fraud there is no

would have perfected the legal business, which would determine the non-existence of legitimation

to process the personal data of the interested party. And this because, once the contract is signed,

the legal basis of the treatment that legitimizes the contractor as controller

to treat the personal data of the owner of these in a contracting of a product

would be the one provided for in art. 6.1.b) of the RGPD.

For this legal basis of art. 6.1.b) of the RGPD exists and legitimizes the treatment

data of the holder necessary for the execution of a contract, it is required that the data

are supplied by their owner, which does not happen when the identity is supplanted. Yes

No, it would be producing a treatment of personal data with respect to a contract or service that has not been requested.

Therefore, to avoid fraud, it must be verified that the contractual consent is provided by the true owner of the data, and must perform the contractor due diligence in the process of identification and verification of identity of the contracting person. The SAN of April 29, 2010 considers that "the question (...) is not so much to elucidate whether the appellant processed the personal data of the complainant without their consent, such as whether or not they used reasonable diligence in of trying to identify the person with whom he signed the financing contract".

Identity theft is a risk considered specifically by the legislator, according to recital 75 of the RGPD and art. 28 of the LOPDGDD, which imposes those responsible for processing the deployment of all due diligence to eradicate it or minimize it, within the framework of its proactive responsibility. This risk implies important risks, consequently greater diligence, greater reinforcement of security measures security (considering 94 of the RGPD in relation to the mitigation of damages) for obtain a valid contractual consent from its true owner, especially if it can involving minors or vulnerable people.

The correct identification of clients and the adoption of diligent measures to verifying your identity then falls squarely within the scope of data protection personal, because, if not, the risk of identity theft would materialize, which Probable form can materialize in this type of contracting.

Therefore, we can consider that due diligence is the attention of duty legal care.

Being duly diligent implies, in terms of that legal duty of care, preventing
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 does not derive
of his actions, but of his own".
Accordingly, due diligence is made up of four elements: identifying
(assessment of the actual and potential impact of data processing activities);
prevent, mitigate (through follow-up and monitoring) and, finally, be accountable
(communicating the way in which the negative consequences of the
improper data processing). And all this, within a continuous process.
Due diligence, which must be appropriate to the business environments in which
the person responsible for the treatment moves, it includes not only the adoption of measures
techniques and organization appropriate to the treatment in question, but the ability to
prove their compliance.
Therefore, the data controller must "be obliged to apply measures
timely and effective and must be able to demonstrate the conformity of the activities of
treatment with this Regulation, including the effectiveness of the measures. sayings

Measures should take into account the nature, scope, context and purposes of the

treatment, as well as the risk to the rights and freedoms of natural persons.

Recital 74 of the RGPD.

Demonstrating due diligence is essential, not being enough to allege the

absence of fault, because as affirmed by the National High Court, for all the Judgment

278/2015 of June 30, 2015 (Rec. 163/2014), "To the above must be added, following

the judgment of January 23, 1998, partially transcribed in the SSTS of October 9

of 2009, Rec 5285/2005, and of October 23, 2010, Rec 1067/2006, that "although the

culpability of the conduct must also be the object of proof, must be considered in

order to the assumption of the corresponding load, which ordinarily the elements

volitional and cognitive skills necessary to appreciate it are part of the behavior

tested, and that its exclusion requires proof of the absence of such elements,

or in its normative aspect, that the diligence that was required by the person has been used

alleges its non-existence; not enough, in short, to exculpate behavior

typically unlawful the invocation of the absence of fault".

In conclusion, in order to act with due diligence, the data controller

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

adequate to verify the identity of the people whose personal data is going to be processed or

treats (if it subsequently detects, during the treatment, an impersonation of

identity), to ensure, ultimately, that it has legitimacy to deal with such

personal information.

IV

The documentation in the file shows that the defendant violated the

article 6.1 of the RGPD, every time you carried out the treatment and communicated your data

without legitimacy to do so in order to register supply contracts

of energy not requested by the claimant, without having proven that there was

legitimately contracted, had legal coverage for the collection and treatment

of your personal data, or there is any other cause that makes the

treatment carried out.

Consequently, it has carried out a processing of personal data without

accredited that it has the legal authorization to do so.

Article 6.1 RGPD says that the treatment "will be lawful if it is necessary for the

performance of a contract to which the interested party is a party.

It was therefore essential that the respondent accredit before this Agency that the

The claimant had contracted with her the supplies of gas, electricity, in addition to a

maintenance service called Servielectric Xpress.

The respondent did not reply to this Agency, after the requirements made on 18

September and October 6, 2020, nor did it make allegations to the initiation agreement

of this sanctioning procedure.

v

In order to determine the administrative fine to be imposed, the

provisions of articles 83.1 and 83.2 of the RGPD, precepts that indicate:

"Each control authority will guarantee that the imposition of fines

administrative actions under this article for violations of this

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

proportionate and dissuasive."

"Administrative fines will be imposed, depending on the circumstances of each

individual case, in addition to or as a substitute for the measures referred to in article

58, section 2, letters a) to h) and j). When deciding to impose an administrative fine 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

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 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 they have applied in

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 remedy the

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

what measure;

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

related to the same matter, compliance with said measures;

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

personal information.

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

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

commission of the offence.

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

infringement, which cannot be attributed to the absorbing entity.

f) Affectation of the rights of minors.

g) Have, when not mandatory, a data protection officer.

h) Submission by the person in charge or person in charge, on a voluntary basis,

alternative conflict resolution mechanisms, in those cases in which

there are controversies between them and any interested party."

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

fine to be imposed on the defendant, as responsible for an infraction typified in the

article 83.5.a) of the RGPD, the following factors are considered concurrent:

-

The intentionality or negligence of the infraction (art. 83.2 b).

- Basic present identifiers are affected (name, address,

bank account number) (art. 83.2 g)

This is why it is considered appropriate to graduate the sanction to be imposed on the person claimed and set it at the amount of €6,000 for the infringement of article 6.1.b) of the RGPD.

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 CREATOR ENERGY, S.L, with NIF B67301036, for an infringement of Article 6.1b) of the RGPD, typified in Article 83.5.a) of the RGPD, a fine of 6,000 euros (six thousand euros).

SECOND: NOTIFY this resolution to CREATOR ENERGY, S.L, with NIF B67301036.

THIRD: Warn the sanctioned person that he must make the imposed sanction effective once that this resolution is enforceable, in accordance with the provisions of art. 98.1.b) of Law 39/2015, of October 1, of the Common Administrative Procedure of the Public Administrations (hereinafter LPACAP), within the voluntary payment period established in art. 68 of the General Collection Regulations, approved by Real Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003, of 17 December, 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 Spanish Agency of Data Protection in the banking entity CAIXABANK, S.A.. Otherwise, the will proceed to its collection in 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
is between the 16th and last day of each month, both inclusive, the payment term 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 period of one month from the day
following the notification of this resolution or directly contentious appeal
before the Contentious-Administrative Chamber of the National High Court, with
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 two months from the day following the notification of this act,
according to the provisions of 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,
the firm decision may be provisionally suspended in administrative proceedings if the interested party
states its intention to file a contentious-administrative appeal. If this is the
In this case, the interested party must formally communicate this fact in writing addressed to

the Spanish Agency for Data Protection, presenting it through the Registry

Electronic Agency [https://sedeagpd.gob.es/sede-electronica-web/], or through

any of the other records provided for in art. 16.4 of the aforementioned Law 39/2015, of 1

october. You must also transfer to the Agency the documentation that accredits the

effective filing of the contentious-administrative appeal. If the Agency did not have

knowledge of the filing of the contentious-administrative appeal within two

months from the day following the notification of this resolution, I would consider

The precautionary suspension has ended.

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es