 File No.: PS/00099/2022

RESOLUTION OF SANCTIONING PROCEDURE

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

to the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the claimant) dated March 28, 2021

filed a claim with the Spanish Data Protection Agency. The

claim is directed against OES GLOBAL ENERGY S.L. with NIF B01901941 (in

forward, OES). The reasons on which the claim is based are the following:

Indicates that it has gas and energy supply contracts with the company FREE

ENERGY, but you have received an email from OES, whose address matches

that of FREE ENERGÍA, in which documents of withdrawal of some

electricity contracts signed by two other customers, identified by name and

ID.

Provide, along with your claim document:

- Email print dated March 18, 2021 sent by

clientes@oesenergia.com (indicated as being from the SAC Department and

Incidents) to various email addresses including the one of

the complaining party. In this email, it is indicated that the email of a client is attached

requesting the withdrawal of contracts, and provide the name and surname of a

client with 10 CUPS, and name and surname of another client with 2 CUPS. The names

of these two clients are different from that of the claimant.

- Printing of two pages of the annex to the previous email that are the last page of

withdrawals with SUMINISTRADOR IBÉRICO DE ENERGÍA, S.L. – O.E.S.

ENERGÍA (with NIF B67421875) and the two clients that appeared in the email. Of

these two clients appear the following data: name, surname, DNI, CUPS and

handwritten signature.

- Printing of email dated March 26, 2021 sent by the claimant to

datos@oesenergia.com in which you request the deletion of your data because

You have received an email with data from other clients, and attach the previous email from

dated March 18, 2021.

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

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

hereafter LOPDGDD), said claim was transferred to OES so that

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

actions carried out to adapt to the requirements established in the regulations of

Data Protection.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of

October 1, of the Common Administrative Procedure of the Administrations

Public (hereinafter, LPACAP), was not collected by the person in charge; reiterating the

transfer on 05/26/2021 by certified postal mail, it was again returned

for "unknown".

No response has been received to this letter of transfer.

THIRD: On June 28, 2021, in accordance with article 65 of the

LOPDGDD, the claim presented by the claimant party was admitted for processing.

FOURTH: The General Subdirectorate of Data Inspection proceeded to carry out

of previous investigative actions to clarify the facts in

matter, by virtue of the investigative powers granted to the authorities of

control in article 58.1 of Regulation (EU) 2016/679 (General Regulation of

Data Protection, hereinafter GDPR), and in accordance with the provisions of the

Title VII, Chapter I, Second Section, of the LOPDGDD, being aware of the

following extremes:

INVESTIGATED ENTITIES

During these proceedings, the following entity has been investigated:

OES GLOBAL ENERGY S.L. with NIF B01901941 with address in RAMBLA DEL

GARRAF, Nº 76 - 08812 SANT PERE DE RIBES (BARCELONA)

RESULT OF INVESTIGATION ACTIONS

Among other things, the following information is provided:

1. Indication that the incident described by the claimant occurred due to a

specific error when including the email address of the claimant as a recipient of

an internal email from the company.

2. Indication that this incident was not communicated to the AEPD in 72 hours because,

as the security breach had not been detected, the possibility of

notify the AEPD or those affected.

3. Indication that, since there are two people affected and due to the type of data, the incident

does not imply a risk to the rights and freedoms of those affected.

4. Indication that there is no evidence that third parties have accessed the data, apart from the

claimant.

5. Indication that the mail sent by the complaining party was not detected due to a human error; For this reason, OES did not respond to the request for deletion of the claimant until this file was sent to her by the AEPD.

6. Printout of email dated February 17, 2022 sent by juridico@grupovisalia.com to the email of the complaining party in which the indicates that the response is attached to your request to OES. And also attached letter addressed to the claimant with the following content:

In response to your request for data protection, we inform you that, if In accordance with it, OES ENERGÍA has proceeded to process the deletion of your personal data.

Notwithstanding the foregoing, and in accordance with the provisions of article 17.3 RDPG, we will proceed to keep your data for compliance with the legal obligations that may arise from its legal relationship with the company, as well as, where appropriate, to comply with legal requirements.

For all this, and given that OES ENERGÍA, wants to scrupulously respect the exercise of your rights, we inform you that we remain at your disposal for any clarification you need.

FIFTH: On April 4, 2022, the Director of the Spanish Agency for Data Protection agreed to initiate disciplinary proceedings against the claimed party, for the alleged infringement of Article 5.1.f) of the GDPR, typified in Article 83.5 of the GDPR, and Article 32 of the GDPR, typified in article 83.4 of the GDPR

Notified of the initiation agreement, OES submitted a written statement of allegations in which, in synthesis stated:

-That he considers the proposal for an economic sanction disproportionate for the alleged non-compliance with the indicated normative precepts, since the criterion that has

followed by the AEPD when it comes to imposing sanctions for the alleged infringements of the precepts included in articles 5.1.f) and 32 GDPR in other files, diverge established in this Sanctioning Procedure, suffering OES a grievance comparative.

OES adds that it does not fully understand the reason why the proposal for sanction of this Sanctioning Procedure is so high, especially taking into account note that the sanctioning activity of the Administration is subject to the principle of proportionality, and that it understands that the amount of the sanctions imposed has not been seen suitably modulated.

-In this regard, this Agency points out that, although the penalty initially established is within the framework established by articles 83.5 and 83.4 of the GDPR, for violation of articles 5.1.f) GDPR and 32 GDPR, respectively, it is no less true that there are several factors that must be considered when setting the penalty so that it is proportional and appropriate to the infraction that is analyzed in each case. Taking, then, in consideration all the factors, studied the allegations made by

OES in this regard, it can be concluded that it would be appropriate to estimate partially the same in the sense of reducing the amount of the fines initially proposed.

-That one of the principles that governs the sanctioning administrative law is the "non bis in idem" principle, which implies that two or more cannot be imposed

sanctions on the same facts, and that the fact that promotes this Procedure

Sanctioning is the sending, due to a human and punctual error, of an internal email to

a client who was mistakenly put as the recipient of the same.

OES understands that this fact is sanctioned by the AEPD twice, once per

infringement of article 5.1.f) GDPR in relation to non-observance of the principle of

confidentiality and integrity, and another for breach of article 32 GDPR in

regarding the lack of adoption of technical and organizational measures that result

appropriate to guarantee a level of security appropriate to the risk of the treatment,

must be penalized for a single infraction.

-In this regard, it should be noted that Law 40/2015, of October 1, Reg-

Legal Men of the Public Sector (LRJSP) includes the principle NON BIS IN IDEM,

by establishing in its article 31.1:

"Facts that have been criminal or administrative may not be sanctioned.

especially, in the cases in which the identity of the subject, fact and fundamentals is appreciated.

dude".

In this sanctioning procedure, the necessary budgets are not given.

since different facts are imputed, each of them, likewise, has

specified in different articles of the GDPR. The assumption typified in the article

5.1.f) of the GDPR refers to the fact that the personal data of two clients

of OES were exposed to a third party. The assumption typified in article 32

refers to the fact that both the person in charge and the person in charge of the treatment

should take appropriate technical and organizational measures to ensure a

security level appropriate to the risk, concluding that said measures have not

had been adopted in the present case.

-That the facts that have led to the initiation of the Sanctioning Procedure do not

Do they obey, in any case, an intention to break the confidentiality of the data

of OES clients, nor to any other type of intention of OES to breach

with its obligations in terms of data protection, not concurring the necessary

requirement of guilt to be able to impose an administrative sanction since it is

established the jurisprudential criterion that any sanction must be ruled out regardless of

negligent or negligent conduct (principle of guilt in sanctioning matters);

Therefore, they want to show that, in no case, has OES sought a re-

result of the disclosure of the personal data of its clients and that it has only been pro-

filed a claim for these facts, being, as previously mentioned-

mind, due to a human and punctual error.

-In this regard, this agency cites the judgments of the Supreme Court of 12

(rec. 388/1994) and May 19, 1998, Sixth Section, which state that "in the

scope of administrative responsibility, it is not enough for the conduct to be

unlawful and typical, but it is also necessary that he be guilty, that is,

consequence of an action or omission attributable to its author due to malice or

prudence, negligence or inexcusable ignorance (...)"

In the present case it is appreciated that OES is responsible and, therefore, guilty,

in the sense pointed out by the aforementioned sentences, of the imputed infractions

days, without being able to excuse oneself in the lack of intentionality, since there is no room for

doubt that his conduct has been at least imprudent, by sending by mail

e-mail to a client the contracts corresponding to two other people.

nas, contracts containing personal data.

-That, from the moment you became aware of the security breach

that initially gave rise to the Initial Requirement and, subsequently, the

Disciplinary Procedure, has applied the following technical and organizational measures:

you go (in addition to those indicated in the response to the Initial Requirement):

• Implement training courses for employees

• Configuration of the email of all the personnel eliminating the predictive of

autocomplete email

• Study of the feasibility of forwarding email to an external mail server.

terno to carry out filtering of recipients.

-In this regard, this Agency has nothing to object to or add to the measures

days implemented.

SIXTH: On June 1, 2022, a resolution proposal was formulated,

proposing That the Director of the Spanish Agency for Data Protection be

sanction OES GLOBAL ENERGY S.L., with NIF B01901941:

-for an infringement of Article 5.1.f) of the GDPR, typified in Article 83.5 of the

GDPR, with a fine of €25,000 (twenty-five thousand euros).

-for a violation of Article 32 of the GDPR, typified in Article 83.4 of the GDPR,

with a fine of €10,000 (ten thousand euros).

SEVENTH: Notified of the resolution proposal, OES presents a new brief of

allegations dated 08/04/2022, in which all the allegations are considered reproduced

made in previous writings, and adds that:

- In relation to the reasoning presented by the AEPD in response to the allegation

third in the motion for a resolution, does not share that argument for the

following reasons:

1st. The AEPD, on the one hand, indicates that OES cannot be exonerated from its lack of

intentionality, but justifies it in the existence of a conduct that "has been

at least reckless." This part understands that intentionality (deceit) and

recklessness are opposite terms and cannot be malicious conduct

consequence of reckless conduct or, in other words, cannot be

attribute to OES intentional action when the conduct

allegedly originates the fraud in the act is classified as culpable by the person herself

AEPD.

2nd. In any case, the allegedly infringing conduct indicated by the AEPD and

that accuses OES as "reckless", understands this part that could only be

attributable to an alleged violation of OES of article 32 GDPR in relation to the

technical and organizational measures applied to the processing of personal data since,

If applicable, it would correspond to the data controller to design and implement

those that were necessary to safeguard the security of the data

personal treated. However, the fact that in the field of activity

of the company, a worker, recklessly, has made a copy to

the claimant in an email whose recipients should have been

only internal company personnel, constitutes a circumstance that, more

beyond the possible technical and/or organizational measures that OES could have

implemented at the time, is beyond the effective control of the company insofar as it is

a human and punctual error that has consisted of not reviewing the recipients of a

internal email prior to sending.

In view of all the proceedings, by the Spanish Agency for Data Protection

In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: It is proven that the claimant had signed contracts of

gas and energy supply with the company FREE ENERGÍA.

SECOND: It is proven that the claimant received an email

of OES, whose address coincides with that of FREE ENERGÍA, in which are attached

withdrawal documents from some electricity contracts signed by two others

clients, identified with their name and ID.

FUNDAMENTALS OF LAW

Yo

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

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

control authority and as established in articles 47 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."

In relation to the allegations presented to the resolution proposal, OES considers

reproduced those already presented above and adds that:

II

1-In relation to the reasoning presented by the AEPD in response to the allegation

third in the motion for a resolution, does not share that argument, since the

AEPD, on the one hand, indicates that OES cannot be exonerated from its lack of

intentionality, but justifies it in the existence of a conduct that "has been

at least reckless", and they understand that intentionality (deceit) and recklessness are

opposite terms and it cannot be an intentional conduct that is the consequence of a

reckless conduct or, in other words, OES cannot be attributed to having

acted intentionally when the conduct that supposedly originates the fraud in

the action is classified as culpable by the AEPD itself.

-In this regard, this Agency clarifies that at no time has it been attributed to

OES intentionality in the action, but without responsibility, in the given sense

by the sentences cited, Sentences of the Supreme Court of 12 (rec.

388/1994) and May 19, 1998, Sixth Section, which state that "in the

As regards administrative responsibility, it is not enough that the conduct is unlawful.

ridiculous and typical, but it is also necessary that it be guilty, that is, consequential.

consequence of an action or omission attributable to its author due to malice or imprudence.

inexcusable inaccuracy, negligence or ignorance (...)”

2- The allegedly infringing conduct indicated by the AEPD and which it imputes to OES

as "reckless", they understand that it could only be attributable to an alleged

infringement of OES of article 32 GDPR in relation to technical measures and

organizational rules applied to the processing of personal data since, where appropriate, yes

It would correspond to the data controller to design and implement those that

were necessary to safeguard the security of the personal data processed.

However, the fact that in the scope of the ordinary activity of the company, a

worker, recklessly, has copied the claimant in an email

email whose recipients should have been only internal staff of the

company, constitutes a circumstance that, beyond the possible technical measures

and/or organizational that OES could have implemented at the time, escapes the

effective control of the company as soon as it is a human and punctual error that has

consisted of not reviewing the recipients of an internal email prior to its

shipment.

-In this regard, this Agency cites Judgment 188/2022 of the Third Chamber Section

of Administrative Litigation of the Supreme Court, dated 02/15/2022, which in

its foundation of Third Law indicates:

(...) Finally, it is appropriate to remember that legal persons are responsible for the

performance of its employees or workers. For this reason, no

strict liability, but if it is transferable to the legal person the lack of

diligence of its employees, in this sense STC 246/1991, of December 19 f.j 2.

(…)

Article 5.1.f) "Principles relating to processing" of the GDPR establishes:

"1. Personal data will be:

(…)

f) processed in such a way as to guarantee adequate security of the

personal data, including protection against unauthorized processing or

illicit and against its loss, destruction or accidental damage, through the application

of appropriate technical or organizational measures ("integrity and

confidentiality»).”

In the present case, it is clear that there was an improper exposure of the personal data of

customers, registered in the OES database, since they were sent by mail

electronically signed documents containing personal data such as

name, surname and ID, to a third party.

Article 83.5 of the GDPR under the heading "General conditions for the imposition of

administrative fines” provides:

IV.

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 under articles 5, 6, 7 and 9; (…)”

In this regard, the LOPDGDD, in its article 71 "Infractions" establishes that

"The acts and behaviors referred to in sections 4,

5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that result

contrary to this organic law”.

For the purposes of the limitation period, article 72 "Infractions considered very

serious” of the LOPDGDD indicates:

"1. Based on what is established in article 83.5 of Regulation (EU) 2016/679,

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

a substantial violation of the articles mentioned therein and, in particular, the

following:

a) The processing of personal data in violation of the principles and guarantees

established in article 5 of Regulation (EU) 2016/679. (…)”

For the purposes of deciding on the imposition of an administrative fine and its amount,

considers that the infringement in question is serious for the purposes of the GDPR and that

it is appropriate to graduate the sanction to be imposed according to the following criteria that

Article 83.2 of the GDPR establishes:

V

As mitigations:

-The incident affected only three people, and to date no

has verified that they suffered any damage derived from it. (Article

83.2.a)

Likewise, it is considered appropriate to graduate the sanction to be imposed in accordance with the

following criteria established in section 2 of article 76 "Sanctions and measures

corrective measures" of the LOPDGDD:

As aggravating factors:

- Linking the activity of the infringer with the performance of

processing of personal data, since in the case of a company

energy supplier, with numerous customers with whom

they sign contracts, they process a large number of personal data.

(Article 76.2.b)

The balance of the circumstances contemplated in article 83.2 of the GDPR and the

Article 76.2 of the LOPDGDD, with respect to the offense committed by violating the

established in article 5.1.f) of the GDPR, once also examined the

OES allegations, allow a penalty of €25,000 (TWENTY-FIVE THOUSAND

EURO).

Article 32 "Security of treatment" of the GDPR establishes:

SAW

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

nature, scope, context and purposes of processing, as well as risks of

variable probability and severity for the rights and freedoms of individuals

physical, the person in charge and the person in charge of the treatment will apply technical and

appropriate organizational measures to guarantee a level of security appropriate to the risk,

which may include, among others:

a) the pseudonymization and encryption of personal data;

b) the ability to guarantee the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

c) the ability to restore the availability and access to personal data

quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and assessment of effectiveness

technical and organizational measures to guarantee the safety of the

treatment.

2. When evaluating the adequacy of the security level, particular consideration will be given to

take into account the risks presented by data processing, in particular as

consequence of the destruction, loss or accidental or illegal alteration of data

personal information transmitted, preserved or processed in another way, or the communication or

unauthorized access to such data.

3. Adherence to an approved code of conduct pursuant to article 40 or to a

certification mechanism approved under article 42 may serve as an element

to demonstrate compliance with the requirements established in section 1 of the

present article.

4. The controller and the processor shall take measures to ensure that

any person acting under the authority of the controller or processor and

have access to personal data can only process such data by following

instructions of the person in charge, unless it is obliged to do so by virtue of the Law of

the Union or of the Member States.

In the present case, at the time of the breach, OES did not adopt a

minimum of measures aimed at avoiding that, together with the email addresses

e-mail from people belonging to their own organization, to whom they were going

for the withdrawal documents of several CUPS of two clients, it is

include the email address of the complaining party, which is why it ended

receiving documents not originally intended for her, with personal data of

others.

Article 83.4 of the GDPR under the heading "General conditions for the imposition of

administrative fines" provides:

VII

Violations of the following provisions will be sanctioned, in accordance with the

paragraph 2, with administrative fines of maximum EUR 10,000,000 or,

in the case of a company, an amount equivalent to a maximum of 2% of the

total annual global business volume of the previous financial year, opting for

the highest amount:

a) the obligations of the person in charge and the person in charge according to articles 8,

11, 25 to 39, 42 and 43; (…)"

In this regard, the LOPDGDD, in its article 71 "Infractions" establishes that

"The acts and behaviors referred to in sections 4,

5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that result

contrary to this organic law".

For the purposes of the limitation period, article 73 "Infractions considered serious"

of the LOPDGDD indicates:

"Based on what is established in article 83.4 of Regulation (EU) 2016/679,

are considered serious and will prescribe after two years the infractions that suppose a

substantial violation of the articles mentioned therein and, in particular, the

following:

(…)

f) The lack of adoption of those technical and organizational measures that

are appropriate to ensure a level of security appropriate to the

risk of treatment, in the terms required by article 32.1 of the

Regulation (EU) 2016/679.

(…)

For the purposes of deciding on the imposition of an administrative fine and its amount,

considers that the infringement in question is serious for the purposes of the GDPR and that

it is appropriate to graduate the sanction to be imposed according to the following criteria that

Article 83.2 of the GDPR establishes:

As mitigations:

-The incident affected only three people, and to date no

has verified that they suffered any damage derived from it. (Article

83.2.a)

Likewise, it is considered appropriate to graduate the sanction to be imposed in accordance with the

following criteria established in section 2 of article 76 "Sanctions and measures

corrective measures" of the LOPDGDD:

As aggravating factors:

- Linking the activity of the infringer with the performance of

processing of personal data, since in the case of a company

energy supplier, with numerous customers with whom

they sign contracts, they process a large number of personal data.

(Article 76.2.b)

The balance of the circumstances contemplated in article 83.2 of the GDPR and the

Article 76.2 of the LOPDGDD, with respect to the offense committed by violating the

established in article 32 of the GDPR, once also analyzed the allegations

presented by OES, allow setting a penalty of €10,000 (TEN THOUSAND EUROS).

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 OES GLOBAL ENERGY S.L., with NIF B01901941, for a

infringement of Article 5.1.f) of the GDPR typified in Article 83.5 of the GDPR, a

fine of €25,000 (TWENTY-FIVE THOUSAND EUROS)

IMPOSE OES GLOBAL ENERGY S.L., with NIF B01901941, for a violation of the

Article 32 of the GDPR, typified in Article 83.4 of the GDPR, a fine of €10,000

(TEN THOUSAND EUROS)

SECOND: NOTIFY this resolution to OES GLOBAL ENERGY S.L.

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

art. 98.1.b) of Law 39/2015, of October 1, on Administrative Procedure

Common of 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, by means of its income, 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, open in the name of the Agency

Spanish Data Protection Agency at the bank CAIXABANK, S.A.. In the event

Otherwise, it will proceed to its collection in the executive period.

Once the notification has been received and once executed, if the execution date is

between the 1st and 15th of each month, both inclusive, the term to make the payment

voluntary will be until the 20th day of the following or immediately following business month, and if

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

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

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

Resolution will be made public once the interested parties have been notified.

Against this resolution, which puts an end to the administrative process in accordance with art. 48.6 of the

LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the

Interested parties may optionally file an appeal for reversal before the

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

count from the day following the notification of this resolution or directly

contentious-administrative appeal before the Contentious-administrative Chamber of the

National Court, in accordance with the provisions of article 25 and section 5 of

the fourth additional provision of Law 29/1998, of July 13, regulating the

Contentious-administrative jurisdiction, within a period of two months from the

day following the notification of this act, as provided for in article 46.1 of the

referred Law.

Finally, it is noted that in accordance with the provisions of art. 90.3 a) of the LPACAP,

may provisionally suspend the firm resolution in administrative proceedings if the

The interested party expresses his intention to file a contentious-administrative appeal.

If this is the case, the interested party must formally communicate this fact through

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

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

web/], or through any of the other registries provided for in art. 16.4 of the

aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the

documentation proving the effective filing of the contentious appeal-

administrative. If the Agency was not aware of the filing of the appeal

contentious-administrative proceedings within a period of two months from the day following the

Notification of this resolution would terminate the precautionary suspension.

Mar Spain Marti

Director of the Spanish Data Protection Agency

938-120722

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es