 File No.:

RESOLUTION OF TERMINATION OF THE PROCEDURE FOR PAYMENT

VOLUNTEER

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

to the following

BACKGROUND

FIRST: On August 8, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate sanction proceedings against ENDESA ENERGÍA,

S.A.U. (hereinafter the claimed party). Notified the initiation agreement and after analyzing

the allegations presented, on November 14, 2022, the

proposed resolution that is transcribed below:

<<

File No.: EXP202200455

PROPOSED RESOLUTION OF SANCTION 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 claiming party), on December 21,

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

The claim is directed against ENDESA ENERGÍA, S.A.U. with NIF A81948077 (in

below, the claimed party). The reasons on which the claim is based are the following:

following:

The claimant states that, on December 16, 2021, he received in his

address the invoice of the contract that has been maintained for years with the entity

claimed, in the name of a third person (her niece) and that, after contacting the

claimed, was informed that a third party had changed the ownership of the contract, without

Your consent.

Along with the claim, he provides an invoice from December 2021 addressed to his niece and

bank statement, dated November 2021, with the charge to your bank account.

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

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

forward LOPDGDD), said claim was transferred to the claimed party, for

to proceed with 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), by means of electronic notification, was received in

dated January 18, 2022, as stated in the certificate in the file.

In response to the request for an extension of the one-month period that was granted to

to proceed to the analysis of the claim presented, on February 3,

2022, it was agreed to extend it up to a maximum of 10 business days.

On March 4, 2022, this Agency received a written response in the

indicating that on December 16, 2021, the claimant received in his

address the invoice for a contract with Endesa Energía, in the name of a third party

person, associated with the supply point where his father, B.B.B. and in whose name

acts A.A.A., was the holder of a contract with the company Energía XXI Comercializadora

of reference S.L.U. (hereinafter, "Energía XXI"), whose payment was owned by the owner himself.

A.A.A..

It states that, as reflected in Endesa's internal systems

Energy, dated October 21, 2021, the sales channel of Endesa Energía

"Commercial Agents" contacted C.C.C. by telephone, through the supplier

Eastern Andalusia Energy, S.L.U. (hereinafter, "EAO"), who, under a contract of

provision of telemarketing services and acting as the person in charge of the

treatment, makes recruitment calls to potential clients who have previously

given their express consent for this, through the offer of products and

Endesa Energía and Endesa X services.

It states that Endesa Energía has detected anomalous behavior on the part of

your employee since, as it has been found out, the operator did not provide the SMS

correct with the confirmation of contracting of C.C.C., since it did not correspond

with the telephone number confirmed in the call by C.C.C.. In this case,

the operator carried out a change of ownership and marketing company, in

a supply point of which the person in whose name it was registered was not the owner

the contract and, in addition, provided an invalid certified SMS, as acceptance of the

hiring.

Finally, it is indicated that, although the incident was caused by the procedure

of an operator that strayed from the procedure, from the Office of the

Endesa's Data Protection Officer has urged Endesa Energía to,

without prejudice to the ordinary audits that it carries out, reinforce, even more, the

controls regarding the actions carried out by the EAO provider. Also, it

has recommended Endesa Energía to send a warning to EAO indicating the

seriousness of the events that occurred and the damage caused to the interested party.

THIRD: On March 21, 2022, in accordance with article 65 of the

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

FOURTH: On August 8, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate disciplinary proceedings 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 Public Administrations (in



hereafter, LPACAP), for the alleged infringement of article 32 of the GDPR, typified in

Article 83.4 of the GDPR.

The startup agreement was sent, in accordance with the rules established in the Law

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

Public Administrations (hereinafter, LPACAP), by means of electronic notification,

being received on August 10, 2022, as stated in the certificate that works

on the record.

FIFTH: In response to the request for an extension of the term to present

allegations, on August 11, 2022, it was agreed to extend it up to a

maximum of 5 days.

In response to the letter requesting a copy of the referenced file, on December 19,

August 2022, access was given to it.

SIXTH: Notified the aforementioned start agreement in accordance with the rules established in

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

Public Administrations (hereinafter, LPACAP), the claimed party submitted a written

of allegations in which, in summary, he stated that unlawfulness cannot be appreciated in the conduct of Endesa Energía inasmuch as it limited itself to addressing the different C.C.C. contracting requests, among which was the one corresponding to the house located at ***ADDRESS.1, and to facilitate the corresponding procedures for allow the change of ownership of the access contract, following the protocols established, without this entailing allowing access to the personal data of the original holder of the access contract.

It points out that the security measures that Endesa Energía deployed to guarantee the protection of the personal data of the interested parties, they worked correctly since no personal data of any third party was disclosed, and the fact that it was produce an incident in the processing of the contract by providing an SMS invalid confirmation certificate and the sale went ahead, does not imply that Endesa Energía lacks action protocols or procedures and that the security measures have not been adequate to guarantee the protection of the personal data of its customers means, plain and simple, that a operator deviated from the established procedure, providing a certified SMS corresponding to a telephone number of another sale, without this, in any case, has caused any personal data of the clients to have been seen unprotected.

Alternatively, in the event that the main request is not met, it requests, a reduction of the penalty initially set, taking into account the circumstances mitigating measures, specifically, the measures adopted to alleviate any possible detriment to the claimant or the person on whose behalf he acts, as well as to avoid that similar events occur in the future; and the severity and episodic nature of the alleged infringement, since the necessary procedures were initiated to facilitate the replacement of the electricity supply contract for the dwelling in question with the

previous marketing company, as well as the cancellation of the three invoices

emitted by the consumption of energy during the time in which the contract object of

claim was active.



Finally, it points out that the action protocols of the sales channel have been reinforced

"Commercial Agents" and that the facts claimed respond to an event

isolated and punctual, in which only one person has been affected who also

maintained the electricity supply, without having to pay any bill for the

energy consumed and that there has been a failure in the contracting process,

provide an invalid confirmation SMS certificate.

A recording of the telephone call made by the energy provider is provided.

Eastern Andalusia, S.L.U.

SEVENTH: Consequently, not having requested the practice of tests, it is considered

incorporated for evidentiary purposes the documentation provided by the claimant, as well as

such as the allegations to the initiation agreement, all documentation of which

has the claimant.

Of the actions carried out in this procedure and of the documentation

in the file, the following have been accredited:

FIRST: It is established that the claimant was the holder of a contract for the supply of

electricity with the company Energía XXI associated with the supply point located in

***ADDRESS 1.

PROVEN FACTS

SECOND: It is verified that the operator carried out a change of ownership and

trading company, at a supply point of which the person was not the owner

in whose name the contract was registered, providing an invalid certified SMS,

as acceptance of the contract.

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, 48.1, 64.2 and 68.1 of the

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

Guarantee of Digital Rights (hereinafter, LOPDGDD), is competent to

initiate and resolve this procedure, the Director of the Spanish Agency for

Data Protection.

Likewise, article 63.2 of the LOPDGDD determines that: "The 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

In response to the allegations presented by the respondent entity, it should be noted

the next:

In the present case, on October 21, 2021, the Endesa sales channel
Energy "Commercial Agents" contacted C.C.C. by telephone, with the purpose of
to offer you a bonus in contracting the electricity rate. In this way, it
requested through the telephone channel, registration in the electrical supply for the home
of the complaining party, which was processed under the modality "C2-Change of
marketer with modifications in the access contract", in accordance with the
contained in the CNMV Resolution of December 17, 2019.

Regarding the obligations that the claimed party claims for compliance with the
specific regulations of the electricity sector, this instruction has nothing to say beyond
that they cannot suppose in any case a violation of the rest of the
applicable regulations.

The protocol for the management of change of marketer with change of owner
attributes to the incoming marketer the condition of the client's sole interlocutor and
the responsibility of executing all the actions that were necessary for the
change management.

In this sense, it cannot be accepted that, even in order to comply with what is there
established, proceed to obviate the necessary compliance with the regulations on
protection of personal data.

For these purposes, Law 24/2013, of December 26, on the Electricity Sector (hereinafter,
"Law of the Electricity Sector"), establishes the consumer's right to change company
marketer in accordance with the provisions of the European directives of the market
electricity inside.

For this, the regulations establish the general process that must be carried out between the
new marketer or incoming marketer, the distributor and
existing marketer or outgoing marketer. Said change implies the registration of
a new energy supply contract with the incoming retailer and the deregistration

of the existing contract with the outgoing marketer, through an agent who

execute the change, which is the distributor.

Article 46 of the Electricity Sector Law establishes among the obligations of the

marketers, in its section 1 letter g) that of "Formalize the contracts of

supply with consumers in accordance with the regulations that

be applicable". The mention by the Law of the obligation to formalize the contract

among the obligations of the marketers shows that it corresponds to

the marketer and, in the event of a change of marketer, to the

incoming marketer, verify the identity and the voluntary, correct and informed

provision of consent by the consumer, who is his counterpart in the

supply contract.

In this sense, the new marketer (the claimed party) will have to manage

the cancellation of the contract of the claimant with his outgoing marketer, which is carried out

processing your personal data.

Transferring these considerations to the present case, and having been accredited

that the defendant processed the personal data of the claimant, as stated in the

file, the claimed party did not comply with its obligations with due diligence,



because, before activating the procedure to change the supplier, you should

have collected a valid SMS confirmation certificate.

And it is that, as stated in the file, the conduct of the claimed party

led to the violation of article 32 of the GDPR, by carrying out a change of

ownership and marketing company, at a supply point that was not

holder the person in whose name the contract was registered by providing an SMS

invalid certificate, as acceptance of the contract. Thus, it was not verified

adequately the identity of the person who requested the modification of the contract.

The defendant himself in writing dated March 4, 2022 has stated that:

"(...) EAO has informed Endesa Energía that it has detected behavior

anomalous on the part of your employee since, as it has been possible to ascertain, the operator

You did not provide the correct SMS with the confirmation of the hiring of Ms. C.C.C.,

since it did not correspond to the phone number confirmed in the call

by Mrs. C.C.C., (…)"

Therefore, despite the existing security measures, the personal data of the

complaining party were treated by the respondent entity when issuing and sending to its

domicile the invoice of a contract, in the name of a third person. That is, it has

There has been a lack of security measures in the verification of the data of the

person who requested the modification of the contract, therefore the teleoperator in that

moment in which the data was being verified to proceed with the contracting

of the electricity supply with the contracting party, should have been diligent in adopting the precautions

necessary and relevant.

The defendant erred when stating that, simply and simply, an operator moved away from the

established procedure, providing a certified SMS corresponding to a

other sales phone number as security measures need to be taken

in attention to each and every one of the risks present in a data processing of

personal character, including among them, the human factor.

The Supreme Court (Sentences of 04/16 and 22/1991) considers that the element

guilty party, it follows "... that the action or omission, classified as an infraction

administratively punishable, must be, in any case, attributable to its author, for

fraud or imprudence, negligence or inexcusable ignorance.”

For its part, the National Court, in a Judgment of 06/29/2001, in matters of

protection of personal data, has declared that "... the simple

negligence or breach of the duties that the Law imposes on people

those responsible for files or data processing to exercise extreme diligence...".

The Supreme Court has understood that imprudence exists whenever

neglects a legal duty of care, that is, when the offending subject does not

behave with the required diligence. Diligence whose degree of demand will be determined

in view of concurrent circumstances, such as the special value of the property

legal protection and the professionalism required of the offender. In this sense, the Judgment

of 06/05/1998 requires professionals in the sector “...a duty to know

especially the applicable norms”. In similar terms are pronounced the

Judgments of 12/17/1997, 03/11/1998, 03/02 and 09/17/1999.

Applying the previous doctrine, the National Court, in several sentences, among others

those dated 02/14/ and 09/20/2002 and 04/13/2005, require entities that operate in



the data market a special diligence when carrying out the use or

treatment of the same, given that it is the protection of a right

of the people to whom they refer, for which reason their depositaries

must be especially diligent and careful when carrying out operations with

the same and must always opt for the interpretation most favorable to the protection

of the legal assets protected by the norm.

In this regard, the claimed party failed to comply with the legal mandate established in the Article 32 of the GDPR since the security measures were not adequate for guarantee the protection of the personal data of its clients and must be improved after it has been verified that they have not been sufficient to avoid the reported facts.

The defendant also invokes the reduction of the amount of the sanction by reducing the same.

In this regard, it should be noted that taking into account that it is an infringement classified as serious and that in accordance with article 83.4 of the GDPR may be sanctioned “with administrative fines of a maximum of 10,000,000 EUR 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 one with the highest amount,” a significant reduction of this is already applied.

The STS, Chamber 3, of December 16, 2003 (Rec. 4996/98) already indicated that the principle of proportionality of sanctions requires that "the discretion that is granted to the Administration for the application of the sanction to be carried out weighing in any case the concurrent circumstances, in order to achieve the due proportionality between the facts charged and the responsibility demanded".

Principle of proportionality that is not understood to be violated, considering provided the sanction proposed to the entity, for the proven facts and considering the concurrent circumstances, which are detailed below.

Consequently, the allegations must be dismissed, meaning that the arguments presented do not distort the essential content of the offense that is declared committed nor does it imply sufficient justification or exculpation.

II

previous questions

In the present case, in accordance with the provisions of article 4.1 of the GDPR, there is

processing of personal data, since ENDESA

ENERGY, S.A.U. is a company in the electric power trade sector that,

for the development of its electrical production and services activity, carries out

processing of personal data.

It carries out this activity in its capacity as data controller, since it is

who determines the purposes and means of such activity, by virtue of article 4.7 of the GDPR:

"responsible for the treatment" or "responsible": the natural or legal person, authority

public authority, service or other body that, alone or jointly with others, determines the purposes and

means of treatment; if the law of the Union or of the Member States determines

determines the purposes and means of the treatment, the person in charge of the treatment or the criteria



Specific reasons for their appointment may be established by the Law of the Union or of the

Member states.

Article 4 section 12 of the RGPD defines, in a broad way, the "violations of security"

security of personal data" (hereinafter security breach) as "all

those security violations that cause the destruction, loss or alteration

Accidental or illegal transfer of personal data transmitted, stored or processed in

otherwise, or unauthorized communication or access to such data."

In the present case, there is a personal data security breach in the

circumstances indicated above, categorized as a breach of confidentiality,

whenever the claimed entity has allowed access to the personal data of a

client without their consent when carrying out a change of ownership and company

trading company, at a supply point of which the person whose

name the contract was registered, also providing an invalid certified SMS,

as acceptance of the contract.

It should be noted that the identification of a security breach does not imply the impossibility

sanction directly by this Agency, since it is necessary to analyze the

diligence of managers and managers and security measures applied.

The security of personal data is regulated in article 32 of the GDPR, which

regulates the safety of the treatment.

IV.

GDPR Article 32

Article 32 of the GDPR, security of treatment, establishes the following:

"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 ensure the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

c) the ability to restore availability and access to 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.

Recital 74 of the GDPR establishes:

"The responsibility of the data controller must be established for

any processing of personal data carried out by himself or on his behalf. In

In particular, the person responsible must be obliged to apply timely and effective measures

and must be able to demonstrate the compliance of the processing activities with the

this Regulation, including the effectiveness of the measures. These measures must have

into account the nature, scope, context and purposes of the processing, as well as the

risk to the rights and freedoms of natural persons.”

It should be noted that the GDPR in the aforementioned precept does not establish a list of the security measures that are applicable according to the data that is the object of treatment, but it establishes that the person in charge and the person in charge of the treatment apply technical and organizational measures that are appropriate to the risk involved the treatment, taking into account the state of the art, the application costs, the nature, scope, context and purposes of processing, probability risks and seriousness for the rights and freedoms of the persons concerned.

In addition, security measures must be adequate and proportionate to the detected risk, noting that the determination of the technical measures and organizational procedures must be carried out taking into account: pseudonymization and encryption, the ability to ensure confidentiality, integrity, availability and resilience, the ability to restore availability and access to data after an incident, process verification (not audit), evaluation and assessment of the effectiveness of the measures.

In any case, when evaluating the adequacy of the security level, particular account of the risks presented by data processing, such 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 said data and that could cause damages physical, material or immaterial.

In this sense, recital 83 of the GDPR states that:

"(83) In order to maintain security and prevent processing from infringing what provided in this Regulation, the person in charge or in charge must evaluate the risks inherent to the treatment and apply measures to mitigate them, such as the encryption. These measures must ensure an adequate level of security, including the

confidentiality, taking into account the state of the art and the cost of its application
regarding the risks and nature of the personal data to be
protect yourself. When assessing risk in relation to data security, considerations should be
take into account the risks arising from the processing of personal data,
such as the destruction, loss or accidental or unlawful alteration of personal data
transmitted, stored or processed in another way, or communication or access not
authorized to said data, susceptible in particular to cause damages
physical, material or immaterial.

The responsibility of the defendant is determined by the lack of measures of
security, since it is responsible for making decisions aimed at implementing
effectively the appropriate technical and organizational measures to guarantee a
level of security appropriate to the risk to ensure the confidentiality of the data,
restoring their availability and preventing access to them in the event of an incident
physical or technical

In the specific case under review, the security measures failed when processing the
modification of the contract without adequately verifying the personality of the person
requested the change, managing to carry out a change of ownership and company
trading company, at a supply point of which the person whose
name the contract was registered, also providing an invalid certified SMS,
as acceptance of the contract.

The known facts constitute an infringement, attributable to the party

claimed, for violation of article 32 GDPR, since the security measures of

the claimed entity are not adequate to guarantee the protection of the data of

personal character of their clients and must be improved after having been

verified that they have not been sufficient to prevent the facts denounced.

Therefore, the accredited facts constitute an infraction, attributable to the

claimed party, for violation of article 32 GDPR.

Classification of the infringement of article 32 of the GDPR

V

The aforementioned infringement of article 32 of the GDPR supposes the commission of the infringements

typified in article 83.4 of the GDPR that under the heading "General conditions

for the imposition of administrative fines" provides:

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:

to)

the obligations of the controller and the person in charge under 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."

SAW

Responsibility

Establishes Law 40/2015, of October 1, on the Legal Regime of the Public Sector, in

Chapter III, relating to the "Principles of the Sanctioning Power", in article 28,

under the heading "Responsibility", the following:

"1. They may only be penalized for acts constituting an administrative offense

physical and legal persons, as well as, when a Law recognizes their capacity to

act, the affected groups, the unions and entities without legal personality and the

independent or autonomous patrimonies, which are responsible for them

title of fraud or fault."

Lack of diligence in implementing appropriate security measures

constitutes the element of guilt.

VII

Sanction

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

provisions of articles 83.1 and 83.2 of the GDPR, precepts that state:

"1. Each control authority will guarantee that the imposition of fines

administrative proceedings under this article for violations of this

Regulations indicated in sections 4, 5 and 6 are in each individual case

effective, proportionate and dissuasive.

2. 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

nature, scope or purpose of the processing operation in question, as well as the number



number of interested parties affected and the level of damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the person in charge or in charge of the treatment to

settle 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, habi-

gives an account of the technical or organizational measures that have been applied by virtue of the

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

determine whether the controller or processor notified the infringement and, if so, to what extent

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

given 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 certification mechanisms.

fications approved in accordance with article 42,

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

as the financial benefits obtained or the losses avoided, directly or indirectly.

mind, through infraction."

For its part, article 76 "Sanctions and corrective measures" of the LOPDGDD

has:

"1. The sanctions provided for in sections 4, 5 and 6 of article 83 of the Regulation

(UE) 2016/679 will be applied taking into account the graduation criteria

established in section 2 of said article.

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) Linking the activity of the offender with the performance of processing

of personal data.

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 process by absorption after the commission

of the infringement, 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) The submission by the person in charge or in charge, with character

voluntary, alternative conflict resolution mechanisms, in those

cases in which there are controversies between those and any

interested."

data.

In accordance with the precepts transcribed, for the purpose of setting the amount of the penalty for

infraction of article 32, it is appropriate to graduate the fine taking into account:



As aggravating factors:

Article 76.2 b) LOPDGDD: "The link between the offender's activity and the performance of

tion of personal data processing".

The business activity of the claimed entity requires continuous treatment of

personal data, both customers and third parties. Also, the entity

claimed performs for the development of its activity, a high volume of treatment

of personal data since it is one of the largest companies in the country in its

business sector or activity.

Considering the exposed factors, the valuation that reaches the amount of the fine

is €50,000 for violation of article 32 of the aforementioned GDPR, regarding security

of the processing of personal data.

VIII

Measures

If the infringement is confirmed, it could be agreed to impose on the person responsible the adoption of adequate measures to adjust its performance to the regulations mentioned in this act, in accordance with the provisions of the aforementioned article 58.2 d) of the GDPR, according to the which each control authority may "order the person responsible or in charge of the processing that the processing operations comply with the provisions of the this Regulation, where appropriate, in a certain way and within a certain specified term…". The imposition of this measure is compatible with the sanction consisting of an administrative fine, according to the provisions of art. 83.2 of the GDPR.

It is noted that not meeting the requirements of this body may be considered as an administrative offense in accordance with the provisions of the GDPR, classified as an infraction in its article 83.5 and 83.6, being able to motivate such conduct the opening of a subsequent administrative sanctioning procedure.

In view of the foregoing, the following is issued

PROPOSED RESOLUTION

That the Director of the Spanish Agency for Data Protection sanctions ENDESA ENERGÍA, S.A.U., with NIF A81948077, for a violation of article 32 of the GDPR, typified in article 83.4 of the GDPR, with a fine of 50,000.00 euros and order the implementation of corrective measures that prevent in the future repeat similar events.

Likewise, in accordance with the provisions of article 85.2 of the LPACAP, you will be informs that it may, at any time prior to the resolution of this procedure, carry out the voluntary payment of the proposed sanction, which will mean a reduction of 20% of the amount of this. With the application of this reduction, the sanction would be established at 40,000.00 euros and its payment will imply the

completion of the procedure. The effectiveness of this reduction will be conditioned by the



withdrawal or waiver of any administrative action or appeal against the

sanction.

In case you choose to proceed to the voluntary payment of the specified amount

above, in accordance with the provisions of the aforementioned article 85.2, you must do it

effective by entering the restricted account number IBAN: ES00-0000-0000-0000-

0000-0000, opened in the name of the Spanish Data Protection Agency, in the

banking entity CAIXABANK, S.A., indicating in the concept: the reference number

of the procedure that appears in the heading of this document and the cause, for

voluntary payment, reduction of the amount of the sanction. You must also send the

Proof of admission to the Sub-Directorate General of Inspection to proceed to close

The file.

By virtue of this, you are notified of the foregoing, and the procedure is revealed.

so that within TEN DAYS you can allege whatever you consider in your defense and

present the documents and information that it deems pertinent, in accordance with

Article 89.2 of the LPACAP.

R.R.R.

INSTRUCTOR

926-181022

>>

SECOND: On November 23, 2022, the claimed party has proceeded to the

payment of the penalty in the amount of 40,000 euros using the reduction

provided for in the motion for a resolution transcribed above.

THIRD: The payment made entails the waiver of any action or resource in the

against the sanction, in relation to the facts referred to in the

resolution proposal.

FOURTH: In the previously transcribed resolution proposal, the

acts constituting an infringement, and it was proposed that, by the Director, the

responsible for adopting adequate measures to adjust its performance to the

regulations, in accordance with the provisions of the aforementioned article 58.2 d) of the GDPR, according to

which each control authority may "order the person responsible or in charge of the

processing that the processing operations comply with the provisions of the

this Regulation, where appropriate, in a certain way and within a certain

specified term…".

FUNDAMENTALS OF LAW

Yo

Competence

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, 48.1, 64.2 and 68.1 of the

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



guarantee of digital rights (hereinafter, LOPDGDD), is competent to

initiate and resolve this procedure the Director of the Spanish Protection Agency

of data.

Likewise, article 63.2 of the LOPDGDD determines that: "The 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

Termination of the procedure

Article 85 of Law 39/2015, of October 1, on Administrative Procedure

Common for Public Administrations (hereinafter, LPACAP), under the heading

"Termination in disciplinary proceedings" provides the following:

"1. Initiated a disciplinary procedure, if the offender acknowledges his responsibility,

The procedure may be resolved with the imposition of the appropriate sanction.

2. When the sanction has only a pecuniary nature or it is possible to impose a

pecuniary sanction and another of a non-pecuniary nature but the

inadmissibility of the second, the voluntary payment by the presumed perpetrator, in

any moment prior to the resolution, will imply the termination of the procedure,

except in relation to the replacement of the altered situation or the determination of the

compensation for damages caused by the commission of the offence.

3. In both cases, when the sanction is solely pecuniary in nature, the

The competent body to resolve the procedure will apply reductions of at least

20% of the amount of the proposed penalty, these being cumulative among themselves.

The aforementioned reductions must be determined in the notification of initiation

of the procedure and its effectiveness will be conditioned to the withdrawal or resignation of

any administrative action or resource against the sanction.

The percentage reduction provided for in this section may be increased

according to regulations."

According to what has been indicated, the Director of the Spanish Agency for the Protection of

Data RESOLVES:

FIRST: DECLARE the termination of the procedure in accordance with the

established in article 85 of the LPACAP.

SECOND: REQUEST ENDESA ENERGÍA, S.A.U. so that within a

month notify the Agency of the adoption of the measures described in the

legal foundations of the proposed resolution transcribed in this

resolution.

THIRD: NOTIFY this resolution to ENDESA ENERGÍA, S.A.U..



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 as prescribed by

the art. 114.1.c) of Law 39/2015, of October 1, on Administrative Procedure

Common of Public Administrations, interested parties may file an appeal

administrative litigation before the Administrative Litigation 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.

Mar Spain Marti

Director of the Spanish Data Protection Agency

1331-281122

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es