 Procedure No.: PS/00054/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: The D. G. OF THE CIVIL GUARD - MAIN POST OF

*** LOCATION.1 (hereinafter, the claimant) dated 08/07/2019 sent an official letter to

the Spanish Agency for Data Protection, in which a letter is attached for possible

violation of data protection regulations. The claim is directed against

ELECTROTECNIA BASTIDA, S.L. with CIF B96466461 (hereinafter, the claimed).

The reasons on which the claim is based are that in a vacant lot of the polygon

industrial area of the town is in a state of abandonment envelopes containing

confidential medical information, containing personal data

corresponding to workers of the claimed.

SECOND: In view of the facts denounced and the documents provided by

the claimant of which this Agency has become aware, the Subdirectorate

General Data Inspection proceeded to carry out actions for the

clarification of the facts in question.

On 10/15/2019, the claim submitted was transferred to the defendant for analysis

and communication to the complainant of the decision adopted in this regard. Likewise, it

required him to send to the determined Agency within a period of one month

information:

- Copy of the communications, of the adopted decision that has been sent to the

claimant regarding the transfer of this claim, and proof that

the claimant has received communication of that decision.

- Report on the causes that have motivated the incidence that has originated the

claim.

- Report on the measures adopted to prevent the occurrence of

similar incidents.

- Any other that you consider relevant.

The respondent has not responded to the request made by the Agency

Spanish Data Protection.

THIRD: On 06/08/2020, in accordance with article 65 of the LOPDGDD, the

Director of the Spanish Agency for Data Protection agreed to admit for processing the

claim filed by the claimant against the respondent.

FOURTH: On 02/12/2021, the Director of the Spanish Protection Agency

of Data agreed to initiate a sanctioning procedure against the defendant, for the alleged

Infraction of article 32.1 of the RGPD, typified in article 83.4.a) of the aforementioned RGPD.

FIFTH: Once the initiation agreement has been notified, the one claimed at the time of this

The resolution has not presented a written statement of allegations, for which reason the

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

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

establishes that in the event of not making allegations within the period established on the

content of the initiation agreement, it may be considered a proposal for

resolution when it contains a precise statement about the responsibility

imputed, reason why a Resolution is issued.

SIXTH: Of the actions carried out in this proceeding, they have been

accredited the following:

PROVEN FACTS

FIRST: On 08/07/2019 the G.C. of ***LOCALIDAD.1 sent an official letter to the AEPD,

in which I attach a letter for possible violation of the regulations on the protection of

data by the claimed, motivated by the abandonment of medical documentation

confidentiality of its workers, in a vacant lot in the industrial estate of the

location.

SECOND: Report provided by the G.C. in which it is pointed out that the patrol of the

post went to the industrial estate taking photographs of the place where

found the documents, collecting the same ones that were transferred to the

barracks; that the documents are 29 envelopes, two of them open, from the Clinic

***CLÍNICA.1 (Management of medicine and prevention, SL) appearing in each of them

the name and surnames of the workers of the respondent who request a "Examination

specific health"; examining one of the envelopes that was open and

inside there are two reports: "Specific health examination" and a second

two-page report of the clinic ***CLINICA.2 of ***LOCALIDAD.2 (Valencia); that

On 06/25/2019, the agent signing the report appeared at the address of the

claimed and identified the administrator of the entity, who was unable to explain

of the abandonment of the documentation of its workers in the wasteland.

It is also recorded in the Report of the list of the 29 people affected

for the facts together with the date of the specific health examination.

THIRD: It consists of a photographic report, providing a general photograph of the

abandoned documentation, 29 envelopes; as well as a detailed photograph of one of the

envelopes bearing the confidential letterhead.

FOUNDATIONS OF LAW

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

control authority, and according to the provisions of articles 47 and 48 of the LOPDGDD,

The Director of the Spanish Agency for Data Protection is competent to initiate

and to solve this procedure.

Yo

Article 58 of the RGPD, Powers, states:

II

"two. Each supervisory authority will have all of the following powers

corrections listed below:

(…)

b) sanction any person responsible or in charge of the treatment with

warning when the treatment operations have infringed the

provided in this Regulation;

(…)”

Article 5 of the RGPD establishes the principles that must govern the treatment

of personal data and mentions among them that of “integrity and confidentiality”.

The cited article states that:

"1. The personal data will be:

(…)

f) treated in such a way as to ensure adequate security of the

personal data, including protection against unauthorized processing or

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

of appropriate technical or organizational measures ("integrity and

confidentiality")".

(…)

III

The denounced facts materialize in the abandonment in a vacant

of the industrial estate of the town of ***LOCALIDAD.1, documentation

containing confidential data of a personal nature, enabling their access to

third parties; data that correspond to workers of the claimed, violating the

data protection regulations.

Article 32 of the RGPD "Security of treatment", establishes that:

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

nature, scope, context and purposes of the treatment, 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 measures and

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

which in your case includes, among others:

a) 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 evaluation of the effectiveness

technical and organizational measures to guarantee the security of the

treatment.

2. When evaluating the adequacy of the security level, particular consideration shall be given to taking into account the risks presented by the processing of data, in particular as consequence of the accidental or unlawful destruction, loss or alteration of data data transmitted, stored or otherwise processed, or the communication or unauthorized access to said data.

3. Adherence to an approved code of conduct under 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 person in charge and the person in charge of the treatment will take measures to guarantee that any person acting under the authority of the controller or the manager and has access to personal data can only process said data following the 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".

The violation of article 32 of the RGPD is typified in the article 83.4.a) of the aforementioned RGPD in the following terms:

"4. Violations of the following provisions will be sanctioned, in accordance with paragraph 2, with administrative fines of a maximum of EUR 10,000,000 or, in the case of a company, an amount equivalent to a maximum of 2% of the global total annual turnover of the previous financial year, opting for the largest amount:

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

11, 25 to 39, 42 and 43.

(…)”

For its part, the LOPDGDD in its article 73, for prescription purposes, qualifies

of “Infringements considered serious”:

“Based on the provisions of 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:

(…)

g) The violation, as a consequence of the lack of due diligence,

of the technical and organizational measures that have been implemented in accordance

to what is required by article 32.1 of Regulation (EU) 2016/679”.

(…)”

The GDPR defines personal data security breaches as

“all those violations of security that cause the destruction, loss or

accidental or unlawful alteration of personal data transmitted, stored or processed

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

IV

From the documentation provided to the file, there are clear indications of

that the claimed party has violated article 32 of the RGPD, when an incident of

security, when documents containing sensitive personal data are abandoned

of workers of the claimed, allowing access to them by third parties with

violation of the established measures.

It should be noted that the RGPD in the aforementioned provision does not establish a list of

the security measures that are applicable according to the data that is

object of treatment, but it establishes that the person in charge and the person in charge of the

treatment will apply technical and organizational measures that are appropriate to the risk

that the treatment entails, taking into account the state of the art, the costs of

application, the nature, scope, context and purposes of the treatment, the risks of

probability and seriousness for the rights and freedoms of the persons concerned.

Likewise, the security measures must be adequate and

proportionate to the detected risk, pointing out that the determination of the measures

technical and organizational information must be carried out taking into account: pseudonymization and

encryption, the ability to ensure the confidentiality, integrity, availability and

resiliency, the ability to restore availability and access to data after a

incident, verification process (not audit), evaluation and assessment of the

effectiveness of the measures.

In any case, when evaluating the adequacy of the level of security,

particularly taking into account the risks presented by the processing of data, such as

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

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data and that could cause damages

physical, material or immaterial.

In this same sense, recital 83 of the RGPD states that:

“(83) In order to maintain security and prevent the treatment from violating the

provided in this Regulation, the person in charge or the person in charge must evaluate

the risks inherent to the treatment and apply measures to mitigate them, such as

encryption. These measures must guarantee an adequate level of security, including
confidentiality, taking into account the state of the art and the cost of its application
regarding the risks and the nature of the personal data that must be
protect yourself. When assessing the risk in relation to data security,
take into account the risks arising from the processing of personal data,
such as the accidental or unlawful destruction, loss or alteration of personal data
transmitted, stored or otherwise processed, or the communication or access is not
authorized to said data, susceptible in particular to cause damages
physical, material or immaterial.
In the present case, as evidenced by the facts and within the framework of the
investigation file E/09606/2019, the AEPD transferred the defendant on
10/15/2019, the claim submitted for analysis requesting the contribution of
information related to the claimed incidence, without it having been received in this
body any response.

The responsibility of the claimed party is determined by the bankruptcy of
security revealed by the claimant, since it is responsible for taking
decisions aimed at effectively implementing technical measures and
appropriate organizational measures to guarantee a level of security appropriate to the risk
to ensure the confidentiality of the data, restoring its availability and preventing
access to them in the event of a physical or technical incident. However, from the
The documentation provided shows that the entity has not only breached this

obligation, but also the adoption of measures in this regard is unknown, despite

of having notified him of the claim filed.

In accordance with the foregoing, it is estimated that the respondent would be

allegedly responsible for the infringement of the RGPD: the violation of article 32,

infraction typified in its article 83.4.a).

In order to establish the administrative fine to be imposed,

observe the provisions contained in articles 83.1 and 83.2 of the RGPD, which

point out:

v

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

administrative actions under this article for violations of this

Regulation 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 as a substitute for 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 will be duly taken into account:

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

nature, scope or purpose of the processing operation in question

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

damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor

to alleviate the damages suffered by the interested parties;

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

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

applied under articles 25 and 32;

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

treatment;

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

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

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

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

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

what extent;

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

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

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

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

certificates approved in accordance with article 42, and

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

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

or indirectly, through infringement.

In relation to letter k) of article 83.2 of the RGPD, the LOPDGDD, in its

Article 76, “Sanctions and corrective measures”, establishes that:

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

2016/679 may also be taken into account:

a) The continuing nature of the offence.

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

of personal data.

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

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

commission of the offence.

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

of the infringement, which cannot be attributed to the absorbing entity.

f) Affectation of the rights of minors.

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

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

voluntary, to alternative conflict resolution mechanisms, in those

assumptions in which there are controversies between those and any

interested."

data.

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

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

article 83.4.a) of the RGPD for which the claimant is responsible, in an assessment

initial, the following factors are estimated concurrent:

The nature and seriousness of the infringement given that it is data

especially sensitive workers of the claimed.

The merely local scope of the treatment carried out by the entity

claimed.

The high number of people whose data has been affected by the

offending behavior (29).

The respondent entity does not record that it has adopted measures to prevent the

produce similar incidents; has not responded to the request

information of the Agency which affects the lack of cooperation with the

control authority in order to remedy the infringement and mitigate the

possible side effects of it.

There is no evidence that the entity had acted maliciously, although

the performance reveals a serious lack of diligence.

The link between the activity of the offender and the performance of treatment of

Personal data.

The claimed entity is a small business.

Therefore, in accordance with the applicable legislation and having assessed the criteria for

graduation of sanctions whose existence has been proven,

The Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE ELECTROTECNIA BASTIDA, S.L., with CIF B96466461, for

an infringement of article 32.1 of the RGPD, typified in article 83.4.a) of the RGPD,

a fine of €3,000 (three thousand euros), in accordance with article 73.g) of the

LOPDGDD.

SECOND: NOTIFY this resolution to ELECTROTECNIA BASTIDA, S.L.,

with CIF B96466461.

THIRD: Warn the sanctioned party that he must make the imposed sanction effective once

Once this resolution is enforceable, in accordance with the provisions of the

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

Common Public Administrations (hereinafter LPACAP), within the payment term
voluntary established in art. 68 of the General Collection Regulations, approved
by Royal Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003,
of December 17, through its entry, indicating the NIF of the sanctioned and the number
of procedure that appears in the heading of this document, in the account
restricted number ES00 0000 0000 0000 0000 0000, opened on behalf of the Agency
Spanish Department of Data Protection in the banking entity CAIXABANK, S.A.. In case
Otherwise, it will be collected in the executive period.

Received the notification and once executed, if the date of execution is
is between the 1st and 15th of each month, both inclusive, the term to carry out the
voluntary payment 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 term of the
payment will be until the 5th of the second following month or immediately after.

In accordance with the provisions of article 50 of the LOPDGDD, the
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
month from the day following the notification of this resolution or directly
contentious-administrative appeal before the Contentious-Administrative Chamber of the
National Court, in accordance with the provisions of article 25 and section 5 of

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

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

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

aforementioned Law.

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

LPACAP, the firm resolution may be provisionally suspended in administrative proceedings

if the interested party expresses his intention to file a contentious appeal-

administrative. If this is the case, the interested party must formally communicate this

made by writing to the Spanish Agency for Data Protection,

introducing him to

the 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 October 1. Also

must transfer to the Agency the documentation that proves the effective filing

of the contentious-administrative appeal. If the Agency were not aware of the

filing of the contentious-administrative appeal within two months from the

day following the notification of this resolution, it would end the

precautionary suspension.

Electronic Registration of

through the

Sea Spain Marti

Director of the Spanish Data Protection Agency