 Procedure No.: PS/00389/2019

RESOLUTION OF PUNISHMENT PROCEDURE

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

based on the following

BACKGROUND

FIRST: On 04/23/2019 the LOCAL POLICE of the BADAJOZ CITY COUNCIL

Filed a complaint against the OUTSIDER LABOR PREVENTION SERVICE

EXTREMEÑA, S.L. (hereinafter the defendant), for alleged infringement of the

regulations on the protection of personal data, when finding scattered on the ground,

next to a company vehicle Extremeña Labor Prevention Service,

SL

medical examination reports dated 12/02/2010 relating to

workers of the company Aguas del Suroeste, S.L.

SECOND: Upon receipt of the claim, the Subdirectorate General for

Data Inspection proceeded to carry out the following actions:

On 05/18/2019, reiterated on 05/30/2019, the claimant was transferred the

claim submitted for analysis and communication to the claimant of the decision

adopted in this regard. Likewise, he was required so that within a month

send certain information to the Agency:

- 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.

On the same date, the claimant was informed of the receipt of the

claim and its transfer to the claimed entity.

On 10/22/2019, in accordance with article 65 of the LOPDGDD, the Director

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

filed by the claimant against the respondent.

THIRD: On 02/24/2020, the Director of the Spanish Protection Agency

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

infringement for the alleged infringement of articles 32.1, 33 and 34 of the RGPD,

sanctioned in accordance with the provisions of article 83.4.a) of the aforementioned RGPD,

considering that the sanction that could correspond would be a WARNING.



FOURTH: 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.

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

accredited the following:

PROVEN FACTS

FIRST: On 04/23/2019 you have entry in the AEPD official of the LOCAL POLICE of the

CITY COUNCIL OF BADAJOZ by which it transfers the Act of complaint against the

EXTREMEÑA LABOR PREVENTION SERVICE, S.L. (hereinafter the

claimed), for alleged infringement of data protection regulations

personal, when found scattered on the ground, next to a company vehicle

External Labor Prevention Service Extremeña, S.L. reconnaissance reports

doctors related to workers of the company Aguas del Suroeste, S.L.

SECOND: A copy of the record of the complaint made by the Police has been provided

Badajoz City Hall No. 10735 indicating: "They are scattered throughout the

ground, next to a company vehicle External Occupational Prevention Service

Extremeña, S.L., medical examination reports dated 12/02/10",

continuing: "The aforementioned medical reports are related to workers of the

company Aguas del Suroeste, S.L. Photocopies of the same are attached.

As a precautionary measure, it is indicated by the Police: "These reports are withdrawn from the road."

THIRD: Copies of the "Reports of the medical examination

Ordinary Periodic practiced in the Occupational Medicine Area of the Service of

Prevention on December 2, 2010 a", relating to two workers of the

company Aguas del Suroeste, S.L.

FOURTH: The respondent has not responded to any of the requirements

formulated by the AEPD; nor has it made allegations to the agreement to start the

penalty procedure.

FOUNDATIONS OF LAW

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

control authority, and as established in art. 47 of the Organic Law 3/2018, of

December 5, Protection of Personal Data and guarantee of rights

Yo

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/12

(hereinafter LOPDGDD), the Director of the Spanish Agency for

Data Protection is competent to resolve this procedure.

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

the Public Administrations, in its article 64 "Agreement of initiation in the

procedures of a sanctioning nature", provides:

II

"1. The initiation agreement will be communicated to the instructor of the procedure, with

transfer of how many actions exist in this regard, and the interested parties will be notified,

understanding in any case by such the accused.

Likewise, the initiation will be communicated to the complainant when the rules

regulators of the procedure so provide.

2. The initiation agreement must contain at least:

a) Identification of the person or persons allegedly responsible.

b) The facts that motivate the initiation of the procedure, its possible

rating and sanctions that may apply, without prejudice to what results

of instruction.

c) Identification of the instructor and, where appropriate, Secretary of the procedure, with

express indication of the system of recusal of the same.

d) Competent body for the resolution of the procedure and regulation that

attributes such competence, indicating the possibility that the alleged perpetrator

can voluntarily acknowledge its responsibility, with the effects provided for in the

article 85.

e) Provisional measures that have been agreed by the body

competent to initiate the sanctioning procedure, without prejudice to those

may adopt during the same in accordance with article 56.

f) Indication of the right to formulate allegations and to the hearing in the

procedure and the deadlines for its exercise, as well as an indication that, in the event

not to carry out

allegations within the stipulated period on the content of the agreement

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

precise statement about the imputed responsibility.

3. Exceptionally, when at the time of issuing the initiation agreement

there are not sufficient elements for the initial qualification of the facts that motivate

the initiation of the procedure, the aforementioned qualification may be carried out in a phase

later by drawing up a List of Charges, which must be notified to

the interested".

In application of the previous precept and taking into account that no

formulated allegations to the initial agreement, it is appropriate to resolve the initiated procedure.

III

Article 58 of the RGPD, Powers, states:

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

corrections listed below:

(…)

i) impose an administrative fine under article 83, in addition to or in

instead of the measures mentioned in this paragraph, depending on the circumstances

of each particular case;

(…)”

The RGPD establishes in article 5 of the principles that must govern the

treatment of personal data and mentions among them that of "integrity and

confidentiality”.

The article notes 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 or unlawful processing and

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

appropriate technical or organizational ("integrity and confidentiality").

In turn, the security of personal data is regulated in articles

32, 33 and 34 of the RGPD.

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".

Article 33 of the RGPD, Notification of a breach of the security of the

personal data to the control authority, establishes that:

"1. In case of violation of the security of personal data, the

responsible for the treatment will notify the competent control authority of

accordance with article 55 without undue delay and, if possible, no later than 72

hours after you become aware of it, unless it is unlikely

that said breach of security constitutes a risk to the rights and

freedoms of natural persons. If the notification to the control authority does not have

place within 72 hours, must be accompanied by an indication of the reasons for

the procrastination

2. The person in charge of the treatment will notify the person in charge without undue delay

of the treatment the violations of the security of the personal data of which

be aware.

3. The notification referred to in section 1 must, at a minimum:

a) describe the nature of the data security breach

including, where possible, the categories and number

approximate number of stakeholders affected, and the categories and approximate number

of affected personal data records;

b) communicate the name and contact details of the data protection delegate

data or another point of contact where further information can be obtained;

c) describe the possible consequences of the breach of the security of the

personal information;

d) describe the measures adopted or proposed by the person responsible for the

processing to remedy the data security breach

including, if applicable, the measures taken to mitigate the

possible negative effects.

4. If it is not possible to provide the information simultaneously, and to the extent

where it is not, the information will be provided gradually without undue delay.

5. The data controller will document any violation of the

security of personal data, including the facts related to it, its

effects and corrective measures taken. Such documentation will allow the

control authority verify compliance with the provisions of this article.



And article 34, Communication of a breach of data security

data to the interested party, establishes that:

"1. When the data security breach is likely

entails a high risk for the rights and freedoms of individuals

physical data, the data controller will communicate it to the interested party without delay

improper.

2. The communication to the interested party contemplated in section 1 of this

article will describe in clear and simple language the nature of the violation of the

security of personal data and will contain at least the information and

measures referred to in article 33, section 3, letters b), c) and d).

3. The communication to the interested party referred to in section 1 will not be

required if any of the following conditions are met:

a) the data controller has adopted technical protection measures

and organizational measures and these measures have been applied to the data

affected by the violation of the security of personal data,

in particular those that make personal data unintelligible for

anyone who is not authorized to access them, such as encryption;

b) the data controller has taken further steps to ensure

that there is no longer the probability that the high risk for the

rights and freedoms of the interested party referred to in section 1;

c) involves a disproportionate effort. In this case, you will choose instead

by a public communication or similar measure by which it is reported

equally effectively to stakeholders.

4. When the person in charge has not yet communicated to the interested party the

violation of the security of personal data, the control authority, once

Considering the probability that such a violation involves a high risk, it may require

to do so or may decide that any of the conditions mentioned in

section 3".

IV

In the present case, it is proven that on 04/23/2019 the LOCAL POLICE

of the CITY COUNCIL OF BADAJOZ provided a copy of the Act of complaint against the

claimed, in which the infringement of the regulations on the protection of

personal data, when found scattered on public roads and next to a vehicle of your

ownership reports of medical examinations relating to workers of the

company Aguas del Suroeste, S.L. containing sensitive data and especially

protected and proceeding the aforementioned forces of order to remove them from public roads

as a precautionary measure.

On the other hand, the lack of sensitivity of the respondent to

the aforementioned facts since it did not respond to the requests for information

made by the AEPD, nor did he respond by submitting a written statement at the beginning of

sanctioning procedure agreement and that, in addition, has the purpose of promoting the



safety and health of workers through the development of activities

necessary and convenient for the prevention of work-related risks.

It should be noted that the GDPR defines data security breaches

personal as “all those security violations that cause the

accidental or unlawful destruction, loss or alteration of transmitted personal data,

stored or otherwise processed, or unauthorized communication or access to

said data”.

From the documentation in the file, there are clear indications of

that the claimed party has violated article 32 of the RGPD, when there was a breach of

security in your systems by allowing and providing access to data

related to medical examination reports dated 12/02/2010 of

workers of the company Aguas del Suroeste who were scattered throughout the

I usually.

The RGPD in the aforementioned precept does not establish a list of security measures.

security that are applicable in accordance with the data that is the object of

treatment, but 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 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.

As indicated previously and in the framework of the file of
investigation ***FILE.1 the AEPD transfer to the claimed on 05/18/2019 and the
05/30/2019 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 Local Police of the City Council of Badajoz, since
who is responsible for making decisions aimed at effectively implementing
appropriate technical and organizational measures to ensure a level of security
appropriate to the risk to ensure the confidentiality of the data, restoring its
availability and prevent access to them in the event of a physical or technical incident.

However, the documentation provided shows that the entity has not only
breached this obligation, but also the adoption of measures to the
respect, despite having notified him of the claim filed.

The RGPD also regulates in its article 33 the notification of violations of
security that may pose a risk to the rights and freedoms of
natural persons to the competent control authority, which in the Spanish case is
of the AEPD.

Therefore, whenever data of a nature is affected in a breach
personnel of natural persons must notify the AEPD and, in addition,
we must notify it within a maximum period of 72 hours from when we have

awareness of the gap.

Lastly, it must be added that having been informed of the incident of

There is also no information on security that he had adopted measures aimed at

remedy it, once he became aware of it.

As there is no evidence that, in accordance with what is stated in the

Article 34 had informed the interested parties of the violation of the security of the

personal data without undue delay once you became aware of them.

In accordance with the foregoing, the respondent would be responsible for the

RGPD violations: the violation of articles 32, 33 and 34, violations

all of them typified in its article 83.4.a).

The violation of articles 32, 33 and 34 of the RGPD are typified

in article 83.4.a) of the aforementioned RGPD in the following terms:

v

"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.

(…)”

The LOPDGDD in its article 71, Violations, states that: "They constitute

infractions the acts and behaviors referred to in sections 4, 5 and 6 of the

Article 83 of Regulation (EU) 2016/679, as well as those that are contrary to the

present organic law".

And in its article 73, for the purposes of prescription, it qualifies as "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 with

required by article 32.1 of Regulation (EU) 2016/679".

r) Failure to comply with the duty to notify the data protection authority

data of a breach of security of personal data in accordance with the

provided for in article 33 of Regulation (EU) 2016/679.

s) Failure to comply with the duty to notify the affected party of a violation of

the security of the data in accordance with the provisions of article 34 of the

Regulation (EU) 2016/679 if the data controller had been required

by the data protection authority to carry out such notification.

The facts revealed in the claim are specified in the

existence of a security breach in the systems of the claimed party allowing the

vulnerability of the same by allowing reports dated 12/02/2010 relating to

medical examinations and belonging to workers of the company Aguas del

Southwest, were scattered on public roads and allowing access to data

contained in them.

All this constitutes a violation of the security of personal data.

which constitutes an infringement of articles 32.1, 33 and 34 of the RGPD.

However, article 58.2 of the REPD provides the following: "Each authority

of control will have all the following corrective powers indicated below:

continuation:

SAW

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

10/12

(…)

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

warning when the processing operations have violated the provisions of

this Regulation;

(…)"

The RGPD, without prejudice to the provisions of its article 83, contemplates in its

article 58.2 b) the possibility of going to the warning to correct the treatments

personal data that do not meet your expectations.

In the case at hand, it has been proven that the defendant did not

has applied technical and organizational measures to guarantee a level of security

capable of guaranteeing the confidentiality, integrity, availability of the

data preventing access; appropriate measures to proceed with the notification in case

of a violation of the security of personal data and the procedure

implemented in the event that the violation of the security of personal data

entails a high risk for the rights and freedoms of natural persons.

The respondent has not responded to the request for information made

by the Inspection Service.

7th

At this point, it is necessary to inform that not meeting the requirements

of the Agency may constitute a very serious infringement in accordance with the

indicated in article 72 of the LOPDGDD, which establishes: “1. Depending on what

established in article 83.5 of Regulation (EU) 2016/679 are considered very serious and

Infractions that suppose a substantial violation will prescribe after three years.

of the articles mentioned therein and, in particular, the following:

(…)

ñ) Failure to facilitate access by data protection authority personnel

competent to personal data, information, premises, equipment and means of

treatment that are required by the data protection authority for the

exercise of its investigative powers.

o) The resistance or obstruction of the exercise of the inspection function by the

competent data protection authority.

(…)”

At the same time, notification of the start agreement and after the term granted

to formulate allegations, I do not present any writing.

As indicated previously, it has been proven that the defendant

has not adopted technical and organizational measures that guarantee a level of

adequate security capable of ensuring the confidentiality, integrity and availability

of the data avoiding its access, loss, etc.; appropriate measures to proceed with the

notification in the event of a personal data breach and the

procedure implemented in the event that the breach of data security

personal entails a high risk for the rights and freedoms of individuals

physical..



It is necessary to point out that if these incidents are not corrected by adopting the

appropriate technical and organizational measures adapting them to what is indicated in the

articles 32.1, 33 and 34 of the RGPD or reiterate the conduct revealed in

the claim and that is the cause of this procedure, as well as not informing

following this AEPD of the measures adopted could give rise to the exercise of

possible actions before the person in charge of the treatment so that they are applied

effectively the appropriate measures to guarantee and not compromise the

confidentiality of personal data and the right to privacy of

people.

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 OUTSIDE LABOR PREVENTION SERVICE

EXTREMEÑA, S.L., with NIF B06307748, for violation of articles 32.1, 33 and 34

of the RGPD, typified in accordance with the provisions of article 83.4.a) of the aforementioned RGPD,

a warning sanction.

SECOND: REQUIRE OUTSIDE LABOR PREVENTION SERVICE

EXTREMEÑA, S.L. with NIF B06307748, so that within a month from the

notification of this resolution, prove: the adoption of security measures

necessary and pertinent in accordance with the regulations on the protection of

personal data in order to prevent recurrence in the future

incidents such as those that have given rise to the claim, correcting the effects of the

violation of access to data, adapting the aforementioned measures to the requirements

contemplated in article 32.1 of the RGPD; the measures taken to proceed with

notification in the event of a personal data breach

in accordance with the provisions of article 33 of the RGPD and the procedure implemented to

the event that the violation of the security of personal data entails a high

risk to the rights and freedoms of natural persons, in accordance with the

indicated in article 34 of the RGPD.

THIRD:

EXTREMEÑA LABOR PREVENTION, S.L. with NIF B06307748.

NOTIFY this resolution to the EXTERNAL SERVICE OF

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